СЕКЦИЯ 7

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

СОДЕРЖАНИЕ

ОБЕСПЕЧЕНИЕ КАЧЕСТВА ПОДГОТОВКИ УЧАЩИХСЯ 9 КЛАССА К ОГЭ ПО ИНФОРМАТИКЕ Антипин В.В., Уткина Т.И., д-р пед. наук, профессор . 1792

МАССОВЫЕ ОТКРЫТЫЕ ОНЛАЙН КУРСЫ (МООК) ОБРАЗОВАТЕЛЬНОГО ПРОСТРАНСТВА: ОЦЕНКА КАЧЕСТВА И ПЕРСПЕКТИВЫ РАЗВИТИЯ Анциферова Л.М., канд. пед. наук, Мячина Ю.В. 1799

МЕТОДИКИ НАЧАЛЬНОГО ИЗУЧЕНИЯ БЕСПИЛОТНОГО МОБИЛЬНОГО ОБЪЕКТА КАК ОБЪЕКТА ИНФОРМАТИЗАЦИИ В УСЛОВИЯХ КАФЕДРЫ ВУЗА Аралбаев Т. З., д-р техн. наук, профессор, Галимов Р. Р., канд. техн. наук, Абрамова Т. В., Каменева Е. В., Халин Г. А. 1805

ПРИМЕНЕНИЕ МАКРОСОВ ТАБЛИЧНОГО ПРОЦЕССОРА В ЗАДАЧЕ ИЗУЧЕНИЯ ИМИТАЦИОННОЙ МОДЕЛИ МОНИТОРИНГА ПЕРЕМЕЩЕНИЯ МОБИЛЬНОГО ОБЪЕКТА В ТРЕХМЕРНОМ ПРОСТРАНСТВЕ Аралбаев Т. З., д-р техн. наук, профессор, Галимов Р. Р., канд. техн. наук, Каменева Е. В., Абрамова Т. В., Захаров Е. Ю. 1813

ПРИМЕНЕНИЕ ПАКЕТА NIST STS ДЛЯ РЕШЕНИЯ УЧЕБНЫХ ЗАДАЧ ДИСЦИПЛИНЫ «ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ» Благовисная А.Н., Самойлов Е.И.*, Давлетбаев А.Ф. 1820

ПРИМЕНЕНИЕ СИСТЕМЫ SAGE ДЛЯ ПОИСКА АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ БУЛЕВЫХ ФУНКЦИЙ И ОТОБРАЖЕНИЙ Благовисная А.Н., Симуськова И.О. 1825

УЧЕБНО-МЕТОДИЧЕСКИЕ ПРИМЕРЫ ПОСТРОЕНИЯ РАДИКАЛОВ КОЛЕЦ Благовисная А.Н., Горелик А.А. 1832

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛЕЙ РАЗНОЧАСТОТНЫХ ВРЕМЕННЫХ РЯДОВ НА ПРИМЕРЕ УРОЖАЙНОСТИ ЗЕРНОВЫХ КУЛЬТУР Болодурина И.П., д-р. техн. наук, профессор, Парфёнов Д.И., канд. техн. наук, Пивоварова К.В. 1836

НАДЕЖНОСТЬ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ Бурькова Е. В., канд. пед. наук, доцент 1843

ПЕЧАТНЫЕ ПЛАТЫ В КУРСОВОМ ПРОЕКТИРОВАНИИ ПО ИНЖЕНЕРНОЙ И КОМПЬЮТЕРНОЙ ГРАФИКЕ Ваншина Е.А., канд. пед. наук, доцент, Ваншин В.В., канд. с.-х. наук, доцент 1848

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ОТ BOT NET Викулов Д.В., Влацкая И.В., канд. техн. наук, доцент 1852

ИСПОЛЬЗОВАНИЕ ИНТЕРАКТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ПОДГОТОВКИ БУДУЩИХ IT-СПЕЦИАЛИСТОВ Глотова М.И., канд. пед. наук, доцент 1856

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ МАТЕМАТИКИ НА ТЕХНИЧЕСКИХ СПЕЦИАЛЬНОСТЯХ В УНИВЕРСИТЕТСКОМ КОЛЛЕДЖЕ ОГУ Гурьянов А.А. 1860

МАТЕМАТИЧЕСКИЙ КРУЖОК КАК ФОРМА РАЗВИТИЯ ИНТЕРЕСА ОБУЧАЮЩИХСЯ К МАТЕМАТИКЕ Колобов А.Н., канд. техн. наук, доцент 1863

РОЛЬ ТЕКСТОВЫХ ЗАДАЧ В МАТЕМАТИЧЕСКОМ ОБРАЗОВАНИИ Колобов А.Н., канд. техн. наук, доцент 1867

ФАКУЛЬТАТИВНЫЕ КУРСЫ ПО МАТЕМАТИКЕ КАК ФОРМА РАЗВИТИЯ МАТЕМАТИЧЕСКИХ СПОСОБНОСТЕЙ Колобов А.Н., канд. техн. наук, доцент 1872

ИСПОЛЬЗОВАНИЕ ДИАГРАММ ДЕЯТЕЛЬНОСТЕЙ В ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ Кузниченко М.А. 1877

МАСШТАБИРОВАНИЕ ОБЛАЧНЫХ СЕРВИСОВ ДЛЯ МУЛЬТИОБЛАЧНОГО ЦЕНТРА КОЛЛЕКТИВНОГО ДОСТУПА Полежаев П.Н., Легашев Л.В. 1882

ПРИМЕНЕНИЕ БАЛЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЫ КАК ФАКТОР ПОВЫШЕНИЯ МОТИВАЦИИ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ ПРИ ИЗУЧЕНИИ МАТЕМАТИКИ Максименко Н.В. 1889

АКТУАЛЬНЫЕ ПРОБЛЕМЫ АВТОМАТИЗАЦИИ АДМИНИСТРИРОВАНИЯ СЕТЕВОГО ОБОРУДОВАНИЯ С УЧЕТОМ НАГРУЗКИ ВИРТУАЛЬНЫХ СЕРВЕРОВ Мельников А.Е., Тагирова Л.Ф., канд. пед. наук, доцент 1895

ВНУТРЕННИЕ ИДЕАЛЫ АЛГЕБР ЛИ И ИХ СВОЙСТВА Мещерина Е.В., канд. физ.-мат.наук 1902

АЛГЕБРАИЧЕСКИЕ МЕТОДЫ КРИПТОАНАЛИЗА В УЧЕБНОМ КУРСЕ «ОСНОВЫ КРИПТОАНАЛИЗА» Михляева А.В., Благовисная А.Н. 1910

ЧТО ТАКОЕ БЛОКЧЕЙН И ЧЕМ ЕГО ТЕХНОЛОГИЯ ОТЛИЧАЕТСЯ ОТ БАЗЫ ДАННЫХ Мучкаева Е.А., Мурзаханова Э.И. 1917

О ЦЕЛЕСООБРАЗНОСТИ ИСПОЛЬЗОВАНИЯ ЛЕКЦИОННЫХ ЗАНЯТИЙ ПРОПЕДЕВТИЧЕСКОГО ХАРАКТЕРА ПРИ ИЗУЧЕНИИ МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН ГУМАНИТАРНЫХ НАПРАВЛЕНИЙ Павленко А.Н., канд. физ. – мат. наук, доцент, Пихтилькова О.А., канд. физ.-мат. наук, доцент 1920

ЗАДАЧА ОБОБЩЕННОЙ СОПРЯЖЕННОСТИ СЛОВ В КЛАССЕ ГРУПП С ОДНИМ ОПРЕДЕЛЯЮЩИМ СООТНОШЕНИЕМ Пихтилькова О.А., канд. физ.-мат.наук, доцент, Павленко А.Н, канд. физ.-мат.наук, доцент 1924

ОБ ОДНОМ АЛГОРИТМЕ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ЭНДОМОРФНОЙ СВОДИМОСТИ Пихтилькова О.А., канд. физ.-мат.наук, доцент, Кравцова А.В. 1929

МОДЕЛИРОВАНИЕ ПРИЛОЖЕНИЙ ДЛЯ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ Полежаев П.Н., Бахарева Н.Ф., д-р техн. наук, профессор, Шухман А.Е., канд. пед. наук, доцент, Ушаков Ю.А., канд. техн. наук, доцент, Легашев Л.В. 1935

ОБЗОР ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ Прокофьев А. В. ... 1940

ИСПОЛЬЗОВАНИЕ МУЛЬТИМЕДИА ТЕХНОЛОГИЙ В ПРОЦЕССЕ ОБУЧЕНИЯ КАК ФАКТОР ПОВЫШЕНИЯ УРОВНЯ ОБРАЗОВАНИЯ СТУДЕНТОВ Ряполова Е.И., канд. пед. наук, доцент 1948

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ПОСТРОЕНИЯ ДЕРЕВА ПРИНЯТИЯ РЕШЕНИЙ Симченко Н. Н., канд. пед. наук, доцент 1952

МАТЕМАТИЧЕСКОЕ ОБРАЗОВАНИЕ В СОВРЕМЕННОМ ОБЩЕСТВЕ Смирнова Е.Н. 1961

ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ, ПРЕДСТАВЛЯЮЩИЕ ПРОЦЕСС И РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ СТУДЕНТОМ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ ПО МАТЕМАТИКЕ Смирнова Е.Н., Томина И.П. 1964

ДИДАКТИЧЕСКИЕ ОСНОВЫ ПРИМЕНЕНИЯ ОБУЧАЮЩЕЙ СРЕДЫ MOODLE ПРИ ИЗУЧЕНИИ МАТЕМАТИКИ В УНИВЕРСИТЕТЕ Тарасова Т.Н. канд. пед. наук, доцент, Руцкова И.Г. 1968

ИНТЕРНЕТ-СЕРВИСЫ КАК СРЕДСТВО РАЗРАБОТКИ КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫХ ЗАДАНИЙ Токарева М.А., канд.техн.наук, доцент, Кулантаева И.А., канд.пед.наук 1972

МОДЕЛЬ РАСПРЕДЕЛЕННОЙ ГЕТЕРОГЕННОЙ МУЛЬТИОБЛАЧНОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ И ПЛАТФОРМЫ АВТОМАТИЗАЦИИ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ ДЛЯ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ Ушаков Ю.А., канд. техн. наук, доцент, Бахарева Н.Ф., д-р техн. наук, профессор, Полежаев П.Н., Шухман А.Е., канд. пед. наук, доцент 1980

ПРИМЕНЕНИЕ ЗАДАЧИ ОБУЧЕНИЯ С ОШИБКАМИ В ПОСТКВАНТОВОЙ КРИПТОГРАФИИ Фадеев С.В. 1992

ОБЗОР ИСТОЧНИКОВ ПО ТЕМЕ МОНИТОРИНГА МОБИЛЬНЫХ ОБЪЕКТОВ Фаткуллина Р.Р. 2000

НЕКОТОРЫЕ АСПЕКТЫ ВНЕДРЕНИЯ ИНТЕРАКТИВНЫХ МЕТОДОВ ОБУЧЕНИЯ БАКАЛАВРОВ НАПРАВЛЕНИЯ ПОДГОТОВКИ «МАТЕМАТИКА И КОМПЬЮТЕРНЫЕ НАУКИ» Шакирова Д.У., канд. пед. наук, Усова Л.Б., канд. пед. наук 2005

ИСПОЛЬЗОВАНИЕ UML-ДИАГРАММ КЛАССОВ ДЛЯ ПОСТРОЕНИЯ ОБЪЕКТНЫХ МОДЕЛЕЙ ДАННЫХ ЭКОНОМИЧЕСКИХ ПРИЛОЖЕНИЙ НА ПЛАТФОРМЕ «1С:ПРЕДПРИЯТИЕ» Широбокова С.Н., канд. экон. наук, Сериков О.Н. 2010

ОБЕСПЕЧЕНИЕ КАЧЕСТВА ПОДГОТОВКИ УЧАЩИХСЯ 9 КЛАССА К ОГЭ ПО ИНФОРМАТИКЕ

Антипин В.В., Уткина Т.И., д-р пед. наук, профессор
Орский гуманитарно – технологический институт (филиал) ОГУ

Понятие «качество» с философских позиций развивалось давно, на протяжении тысячелетий. В настоящее время качество пронизывает практически все аспекты деятельности человека на всех уровнях жизни: личном, общественном, государственном, мировом. Для более четкого понимания любого понятия люди пытаются в словесной форме выразить сущность и свойства описываемого объекта[1].

Качество – видовое отличие сущности (Аристотель)

Связь качества с количеством и мерой (Гегель)

Существуют не качества, а вещи, обладающие качествами, и при том бесконечно многими качествами (Энгельс)

С философских позиций качество означает существенную определенность рассматриваемого объекта, благодаря которому он становится специфическим и отличается от другого объекта[2].

Категория качества выражает соответствующую ступень познания человеком объективной реальности. Первым исследователем категории «качество» принято считать греческого философа Аристотеля (384–322 гг. до н. э.), который дал ее определение[3]. Аристотель рассматривал качество в значениях: как видовое отличие сущности, характеристику состояния сущности, свойство вещи. Рассматривая данные значения понятия «качество» Аристотель в разных работах дает следующие определения.

1. «Качеством, с одной стороны, называется видовое отличие сущности, как например, человек есть некоторое качественно определенное животное двуногое, а конь – четвероногое; и круг – некоторая качественно определенная фигура, ибо это – фигура без углов, так что качеством является относящееся к сущности видовое отличие»[4].

2. Качество – состояние сущностей, находящихся в движении, например, теплота и холодность, белизна и чернота, тяжесть и легкость, и равно другие «определения»[5].

3. «О сходном и несходном говорится только по отношению к качествам. Один предмет не является сходным с другим, кроме как поскольку он дается качественно определенным. Поэтому отличительным признаком качества можно считать то обстоятельство, что о сходном и несходном говорится лишь в применении к нему»[6].

Из этих определений, данных Аристотелем, видно многообразие, множественность отличий объектов, т. е. необходимость, с одной стороны, качественно различать предметы, а с другой – о возможности их объединения в видовые (типовые) группы[7].

В русской истории и культуре также рассматривалось понятие качества, в основном через призму качественной стороны мировоззрения, ментальности, души русского народа. Качественные проявления в бытовой жизни и взаимодействии с другими людьми были сформулированы еще Владимиром Мономахом (1053–1125) в книге «Поучение»[3]. В этой книге Владимир Мономах изложил правила-наставления, охватывающие проблемы общественные, государственные и глубоко личные. «В дому своем не ленитесь, но за всем наблюдайте. Лжи остерегайтесь, и пьянства, и блуда, от того ведь душа погибает и тело. Куда бы вы ни держали путь по своим землям, не давайте отрокам причинять вред ни своим, ни чужим, ни селам, ни посевам, чтобы не стали проклинать вас. Куда же пойдете и где остановитесь, напоите и накормите нищего, более всего чтите гостя, откуда бы он ни пришел. Больного навестите, покойника проводите, ибо все мы смертны. Не пропустите человека, не поприветствовав его, доброе слово ему молвите»[5].

С началом книгопечатания на Руси появляются первые документы с описанием различных технологий и рецептур. Впервые они систематизированы в «Домострое», настоящей энциклопедии домашнего хозяйства того времени. Первая его редакция была составлена в Новгороде в конце XV–XVI веков – начале XVII века. «Домострой» состоит из трех частей: в первой содержатся религиозные наставления, во второй – указания о семейных отношениях, а третья посвящена надлежащему ведению хозяйства[8].

Вопросы, связанные с качеством, в своих трудах поднимали русские философы Владимир Соловьев (1853–1900) «О добродетелях», Петр Струве (1870–1944), Максим Горький (1868–1936) «Полвека для книги», Илья Мечников (1845–1916) «Наука и нравственность», Владимир Вернадский (1863–1945) «Задачи высшего образования нашего времени» и «Философские мысли натуралиста», Николай Бердяев (1874–1948) «О культуре» и «Духовное состояние мира», Лев Толстой (1821–1910) «В чем моя вера», Федор Достоевский (1821–1881) «Дневник писателя»[3].

Более других вопросам качества в развитии всех сторон российской жизни: хозяйства, политики, культуры, образования, воспитания, профессиональной деятельности посвятил русский философ Иван Ильин. Иван Ильин считал, что качество должно стать национальной идеей России. «Русскому человеку есть только один исход и одно спасение – возвращение к качеству и его культуре, ибо количественные пути исхожены, выстраданы и разоблачены, и количественные иллюзии на наших глазах изнашиваются до конца … Верим и знаем: придет час, и Россия восстанет из распада и унижения и начнет эпоху нового расцвета и величества. Но возродится она и расцветет лишь после того, как русские люди поймут, что спасение надо искать в качестве!»[5].

В XX веке с появлением и развитием понятия управление и менеджмент как научного направления, а впоследствии как самостоятельного направления управления качеством и менеджмента качества, количество различных определений качества изменялось содержатель- но. Гуру качества (Деминг, Джуран и др.) дают свои определения данного понятия. Свои определения

качества дают и производственные предприятия. В 70-х годах при традиционном подходе к управлению деятельностью в корпорации Ford было принято следующее определение качества[9]:

«Качество – это соответствие всем необходимым техническим требованиям, которые определены в рабочих чертежах, технических условиях и других подобных документах».

Но уже в конце 80-х годов при развитии взаимоотношений с потребителями и, в первую очередь, благодаря успехам японских фирм, корпорация Ford приняла другое определение качества:

«Качество определяется покупателем; покупатель хочет иметь изделия и услуги, которые в течение всего срока их службы удовлетворяют его или ее потребностям и ожиданиям по цене, соответствующей ценности».

В период последних десятилетий XX века появляются определения термина «качество», установленные в стандартах:

− ГОСТ 15467–79: «качество продукции – совокупность свойств, обуславливающих ее пригодность удовлетворять определенные потребности в соответствии с ее назначением»;

− ИСО 8402–94: «качество – совокупность характеристик объекта, относящихся к его способности удовлетворить установленные и предполагаемые потребности»;

− ИСО 9000:2000: «степень, с которой совокупность собственных характеристик выполняет требования».

Обеспечение качества это тщательное планирование процессов и предоставление доказательств того, что процессы систематически выполняются согласно установленным программам, помогают получить такую уверенность. Для получения этой уверенности потребуется некоторое подтверждение соответствия выполняемых работ программам и адекватности этих программ требованиям. Иногда подобные подтверждения могут привести к выводу о необходимости изменения или обновления программ. Эта фундаментальная концепция основана на так называемом цикле Деминга («Demingwheel»).

ISO 9000: 2000 приводит следующее определение «обеспечения качества»: «часть менеджмента качества, направленная на создание уверенности, что требования к качеству будут выполнены».

Это определение касается не только уверенности потребителя. Очевидно, что обеспечение качества преследует внутреннюю и внешнюю цели[10]

Внутренний аспект здесь таков: обеспечение качества внутри организации дает уверенность руководству. Уверенность в том, что существует понимание требований потребителей и имеется возможность соответствовать этим требованиям при минимально возможных затратах, получая, таким образом, постоянную выгоду.

Внешний аспект: обеспечение качества внутри организации вызывает доверие у потребителя.

Управление качеством и обеспечение качества

Принято считать, что обеспечение качества заменяет управление качеством. Фактически, это не так. Если мы рассмотрим определение менеджмента качества, нам станет очевидно, что в нем говорится и об Управлении Качеством и об Обеспечении Качества; более того, на практике некоторые действия по управлению качеством и действия по обеспечению качества взаимосвязаны.

«Управление качеством» (ISO 9000 : 2000) определяется следующим образом: «Часть менеджмента качества, направленная на выполнение требований к качеству»[11].

Управление качеством включает методы и виды деятельности оперативного характера, направленные и на мониторинг процессов и на устранение причин неудовлетворительной работы на всех этапах петли качества для достижения экономической эффективности. Управление качеством имеет реактивный характер. Для оценки выполнения работ применяются такие методы, как проверки, мониторинг характеристик продукции, мониторинг процесса и т.п., часто с применением статистических методов. Если требования не выполняются, то для устранения причин выполняются корректирующие действия.

Обеспечение качества, наоборот, имеет предупредительный характер. Это система, разработанная для управления деятельностью на всех этапах от продажи, проектирования, закупок и производства до доставки и обслуживания. Ее цель - предотвращение проблем по части качества и обеспечение внедрения качества в продукцию. Обеспечение качества процессов носит восходящий характер, а управление качеством - нисходящий.

Эффективный менеджмент качества требует системы, включающей как обеспечение качества, так и управление качеством. Человеку свойственно ошибаться, и все системы с участием человеческого фактора не могут быть основаны исключительно на предотвращении; они требуют действий по проверке и механизмов корректировки. Человеку свойственно ошибаться, но неразумно повторять ошибки.

Проблема обеспечения качества подготовки учащихся 9 класса ОГЭ по информатике актуализируется требованиями закона об образовании и требованиями ФГОС основного общего образования. В данной работе в качестве средства, обеспечивающего требованиями ОГЭ, выступает электронное учебное пособие.

В основу разработки этого учебного пособия положены выявленные 11 показателей качества подготовки учащихся 9 класса к ОГЭ по информатике:

П1. Понимание процесса подсчета количества информации, П2. Знание о логических операциях, П3. Умение описывать реальные процессы объектов на основе графов, П4. Умение работать с массивами данных в таблицах, П5. Понимание о файловой системе, П6. Знание алгоритмов, П7. Знание кодирования и декодирования информации, П8. Наработка навыков в программировании, П9. Знание перевода систем счисления, П10. Понимание формирования поискового запроса, П11. Знание конъюнкции и дизъюнкции.

Электронное учебное пособие содержит 11 разделов соответствующе 11 показателям:

1.Измерение количества информации

1 задание. Необходимо понимание процесса подсчета количества информации, знание единиц измерения и методики перевода одних единиц в другие. Один символ кодируется 8 битами.

Решение простое: считаем количество всех символов, включая знаки препинания и пробелы, а затем умножаем на количество бит, соответствующих одному символу. И, конечно же, не забываем делать перевод в байты – делим на 8 (столько бит в 1 байте).

15 задание. Задание уровнем сложности, но в целом так же относится к разделу «Измерение информации»

2. Логика

2 задание. Потребуются элементарные знания о логических операциях конъюнкции и дизъюнкции: логическое умножение и сложение. Необходимо выучить эти два определения, чтобы успешно справиться с заданием №2.

3. Формальное описание реальных процессов и объектов

3 задание. Проверка умения анализировать формализованные табличные данные, строить по таблице графы и находить необходимые алгоритмы — как правило, наибольшую или наименьшую длину пути из пункта А в пункт В.

11 задание. Проверяет умение работать с графической информацией, анализировать ее и выдавать верный ответ. Важно не ошибиться в счете, числа обычно очень простые, но их может быть много. Лучше записывать каждый шаг решения.

12 задание. Поиск по готовой базе данных и сформулированному условию

4. Математические инструменты, электронные таблицы

5 задание. Для анализа дается диаграмма. Excel. Главное иметь понятие о том, по каким строкам таблицы построена диаграмма, иначе можно допустить ошибки в решении.

19 задание. Обработка большого массива данных с использование средств электронной таблицы. Знание формул: «сумма», «сумма если», «если», «если и» достаточно, чтобы решить задание.

5. Файловая система

4 задание. Откройте любой документ на вашем компьютере и взгляните в адресную строку, там вы увидите путь к файлу – иерархическая система Windows хранит файлы по принципу «матрешки»: один находится в другом и т.д., пока не дойдем до корневого каталога. Все пройденные нами папки записываются в путь через знак слэша (/).

6. Алгоритм для конкретного исполнителя с фиксированным набором команд

6 задание. Проверка навыков составления и применения уже готового алгоритма, а также немного математики. Скорее всего, потребуется решить простейшее линейное уравнение. Главное – знать, как его составить.

14 задание. Алгоритм для формального исполнителя

16 задание. Алгоритм, записанный на естественном языке, обрабатывающий цепочки символов или списки. Проделывайте каждый шаг алгоритма и

записывайте результат на черновик Не спешите делать все задания устно, будьте предельно внимательны.

7. Кодирование и декодирование информации

7 задание. Имеется шифр, которому в соответствие поставлены буквы нужно либо зашифровать, либо расшифровать целую фразу.

8. Программирование

8 задание. Здесь вовсе не обязательно владеть каким-либо языком программирования, достаточно понимать алгоритмический язык. Задание обычно на линейный алгоритм

9 задание. Задание обычно на простой цикл «пока» или «для».

10 задание. Задание на проверку умения работать с массивами, как правило, одномерными. Необходимо понимание принципа нумерации и нахождения элементов в массиве, а также умение этот массив обрабатывать согласно заданному алгоритму.

20 задание. Проверяются навыки написания простого алгоритма на языке программирования высокого уровня: «Паскаль», «Бейсик», «СИ» и т.д.. Обычно это программа с условием «если», может встретиться простой цикл «для» или «пока».

9. Системы счисления

13 задание. Перевод чисел из одной системы счисления в другую. Обычно двоичная, десятичная, восьмеричная, шестнадцатеричная.

10. ИКТ технологии

17 задание. Связаны с устройством сети Интернет, с адресации в сети, а также с принципом формирования поискового запроса.

11. Поиск информации в Интернете

18 задание. Для успешного решения подобных задач необходимо понимать, что такое конъюнкция и дизъюнкция, а так же их графическое представление с помощью кругов Эйлера.

Разработанное учебное пособие будет подвергнуто экспериментальной проверке на базе 9 классов на предмет эффективности его, относительно обеспечения качества в подготовке учащихся к ОГЭ по информатике.

Список литературы:

1. Философские и социальные аспекты качества : учебное пособие // Б. С. Алешин, Л. Н. Александровская, В. И. Круглов, А. М. Шолом. – М. : Логос, 2004. – 438 с.

2. Алешин, А. Ориентация на потребителя – ключевой фактор успешной деятельно- сти предприятия / А. Алешин // Стандарты и качество. – 2006. – № 5. – С. 38 – 41

3. . Салимова, Т. А. История управления качеством: учебное пособие / Т. А. Салимо- ва, Н. Ш. Ватолкина. – М. : КНОРУС, 2005. – 256 с.

4. Аристотель. Метафизика / Аристотель. – Ростов н/Д. : Феникс, 1999. – С. 73.

5. Антология русского качества / под ред. Б. В. Бойцова, Ю. В. Крянева. – 3-е изд., доп. М. : РИА «Стандарты и качество», 2000. – С. 235.

6. Аристотель. Категории // Этика. Политика. Риторика. Поэтика. Категории / Ари- стотель. – Минск : Литература, 1998. – С. 158.

7. Гличев, А. В. Основы управления качеством продукции. – 2-изд., перераб. и доп / А. В. Гличев. – М. : РИА «Стандарты и качество», 2001. – 424 с. – («Дом качества», вып. 4 (13)).

8. Качество в истории цивилизации. Эволюция, тенденции и перспективы управле- ния качеством / под ред. Дж. Джурана: пер. с англ. О. В. Замятиной и Я. А. Лева. – В 3 т. – Т. 2. – М. : РИА «Стандарты и качество», 2004. – 208 с.

9. Лапидус, В. А. Всеобщее качество (TQM) в российских компаниях / В. А. Лапи- дус. – М. : ОАО «Типография «Новости», 2002. – 432 с.

10. ИСО 9000:2000. Системы менеджмента качества. Основные положения и словарь.

11. ИСО 9000 : 2000. Управление качеством. Руководящие указания по обучению.

МАССОВЫЕ ОТКРЫТЫЕ ОНЛАЙН КУРСЫ (МООК) ОБРАЗОВАТЕЛЬНОГО ПРОСТРАНСТВА: ОЦЕНКА КАЧЕСТВА И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Анциферова Л.М., канд. пед. наук, Мячина Ю.В.
Оренбургский государственный университет

MOOC - Massive Open Online Courses - массовые открытые онлайн курсы - одна из прогрессивных форм дистанционного образования, отношение к которой меняется так же, как и к образованию при помощи сети Интернет. Ещё не так давно, когда только начинали вводить онлайн курсы, онлайн образование относилось к компетенции низкоуровневых и рассматривалось как низкокачественная форма обучения. Однако со временем все чаще признается, что онлайн – один из важных элементов обучения который должен стать значительной частью образования как в высших учебных заведениях, практикующих обучение через Интернет, так и для обеспечения доступности образования наибольшему количеству людей.

Дидактической основой дистанционного образования представляет собой учебный электронный курс. Можно утверждать, что число курсов на абсолютно всех уровнях российского высшего образования приравнивается к числу преподаваемых дисциплин. Множество курсов потенциально готовых и уже применяемых в высшем образовании порождает крайнюю потребность обратится к оценке их качества.

Онлайн курс, подобно классическому очному курсу разрабатывается в соответствии с программой учебной дисциплины, где установлены, помимо остального содержания и цели его освоения. Если в результате обучения на курсе цели были достигнуты, то курс будет оценивается положительно и в для курса будет получена апостериорная оценка качества, а курс рассматривается как «черный ящик». С другой стороны, перед тем как проводить реальное обучение по курсу, необходимо заранее выполнить оценку его качества.

Существуют различные модели учащегося в электронных обучающих системах для оценки курсов. Разные типы моделей могут включать такие параметры, как уровень знаний, скорость и стиль обучения, процент выполнения заданий, выбранные метод/стратегия обучения и т.д. В основном процедуру оценивания проводят с помощью математической обработки совокупности показателей качества курса (например, усреднения) оцененных экспертами. С целью формального выполнения такого рода операции создается базис (массив) ключевых характеристик качества курса, которые оцениваются экспертами. Для этого создается группа, члены который будет проводить оценку. В нее как правило входят специалисты различных направлений: специалисты в оцениваемой области знаний, методисты, психологи и программисты.

Разработка онлайн курса состоит в оптимизации процесса изучения путем подстройки обучающей среды под особенности конкретного ученика. Для осуществления этой цели необходимо найти такое значение, при котором

находится сумма произведения оценок компетентности курса на оценку курсов по критериям. При этом произведение оценок компетентности состоит из произведения относительного коэффициента компетентности на коэффициент развития:

$$z_{ij} = \frac{R_j}{\sum R_{ij}}, \tag{1.1}$$

где R_j - оценка компетентности (коэффициент развития), усреднённая оценка по решаемой проблеме.

На основе экспертной оценки курса пороговое значение успешности курса равняется семидесяти процентам и если коэффициент развития будет иметь значение меньше порогового, то данный курс следует развивать, а иначе курс можно оставить без изменения. Пороговое значение при этом будет изменяться в соответствии с потребностью информационной платформы.

Рассмотрим оценку курсов по критериям:

$$X_{ij} = \sum \alpha_j k_i, \tag{1.2}$$

где X_{ij} – оценка курса по критериям $k_i = \{\mathrm{Re\,z}, Inf, \mathrm{Pr}, Os, Tex\}$; α_j – коэффициент степени доверия.

Для оценки курса формулируются критерии оценок k_i. Которые в свою очередь делятся на объективные и субъективные. Объективная (α_1) - оценка на основании полученной информации о фактических характеристиках оцениваемого объекта, опирающиеся на результаты экспертизы, испытаний или исследований. Субъективная (α_2) - опирается на собственное восприятие оцениваемого объекта, зависящего от мировоззрения, характера и уровня интеллекта, наличия эстетического вкуса и воспитания. При этом коэффициент степени доверия объективной оценки выше субъективной $(\alpha_1 < \alpha_2)$.

К группе объективных оценок относится результативность. Которую можно оценить используя простую модель оценки уровня знаний и метод линейно-кусочной аппроксимации.

К субъективным: информированность, применимость, обратная связь, техническое обеспечение курса. Данную оценку получают из онлайн-опроса после прохождения курса.

Рассмотрим простую модель оценки уровня знаний, которая является наиболее лёгкой и самой распространённой. В ней ответ студента на каждое задание оценивается по двухбалльной (правильно или неправильно) или много балльной (чаще всего пятибалльной) шкале. Оценка выставляется путем вычисления значения *P*.

$$P = \frac{\sum_{i=1}^{k} P_i}{n}, \tag{1.3}$$

где P_i - правильный ответ обучаемого на *i*-е задание; *k*-количество правильных ответов из *n* предложенных *(k<=n)*, которое затем обычно округляется по правилам математики.

Окончательная оценка, как правило, определяется по формуле:

$$L = \begin{cases} 1, P \le c_1 \\ \dots \\ M, P > c_{M-1} \end{cases}, \quad (1.4)$$

где L – окончательная оценка, $c_1 \dots c_M$ – вектор граничных значений, M – максимально возможная оценка (например M=5). К достоинствам данной модели следует отнести простоту ее реализации. В тоже самое время недостатком её является зависимость от количества правильных ответов. Из-за этого она не позволяет объективно оценить знания студента.

Для улучшения оценки знаний был разработан алгоритм основанный на классификации заданий по их дидактическим характеристикам (значимость, трудность, спецификация), который используется в современных онлайн тестированиях. Число баллов, полученных студентом за выполнение n заданий, определяется по формуле:

$$y = \sum_{i=1}^{n} w_i x_i, \quad (1.58)$$

где x_i – оценка за выполнение i-го задания; n – число заданий; $W = w_i$ – вектор весовых коэффициентов заданий, зависящий от их дидактических характеристик.

По завершению контроля определяется средний балл A ($A = \frac{y}{k_n}$), полученный студентом за выполнение n заданий и уточненный средний балл A':

$$A' = A + a_1 \frac{k_n}{n} + a_2 \frac{k_c}{n} + a_3 \frac{k_b}{n}, \quad (1.10)$$

где k_n – количество попыток выполнения n заданий; k_c – количество обращений к справочной информации; k_b – количество заданий, выполненных с превышением отведенного времени $k_b \le n$; a_1, a_2, a_3 – коэффициенты. Далее значения уточненного среднего балла с помощью вектора граничных значений переводятся в обычную пятибалльную шкалу. Параметры контроля, а именно значения весовых коэффициентов w_i, коэффициентов a_i и значения элементов вектора граничных значений определяются на этапе обучения по результатам контрольного эксперимента.

В качестве примера рассмотрим успеваемость студентов по курсу «Математический анализ» представленную в таблице 1.

NAME_DISCIPLINES	STUDENT	PERCENT	TIME_DIFF	PREVISIL_TIME
Математический анализ	259 518	62	3 507	0
Математический анализ	278 061	46	4 086	0
Математический анализ	278 061	61	4 695	0
Математический анализ	332 858	48	4 683	0

Математический анализ	332 858	78	4 437	0
Математический анализ	341 211	57	5 400	0
Математический анализ	347 541	70	5 130	0
Математический анализ	349 543	64	5 013	0
Математический анализ	353 444	72	3 788	0
Математический анализ	379 909	70	1 241	0
Математический анализ	387 964	62	3 149	0
Математический анализ	390 144	77	3 570	0
Математический анализ	399 178	59	1 904	0
Математический анализ	406 790	0	4 199 847	1
Математический анализ	406 790	70	5 331	0
…	…	…	…	…

Таблица 1

После проведения обработки имеющихся данных, учитывая максимальное время прохождения теста, для получения положительной оценки (90 минут) и максимальное количество попыток (3 попытки) были проведены расчёты объективной оценки курса. Применив простую модель уровня знаний, были получены следующие результаты, представленные в таблице 2.

STUDENT	***P***	***L***
662 541	61,67	3
662 349	75,00	4
658 519	77,00	4
640 454	74,00	4
639 191	68,00	3
584 570	77,00	4
584 568	81,67	4
584 554	79,33	4
584 550	68,33	3
584 485	90,00	5
…	…	…

Таблица 3

где P - процент правильности ответа обучаемого на задании; L – окончательная оценка, $c_1...c_M$ – вектор граничных значений, M – максимально возможная оценка (например M=5).

Объективный критерий оценки курса равен:

$$K_{\mathrm{Re}\,z_1} = \frac{L}{\sum_{j=1}^{m} L_j} = 62.20 \qquad (1.11)$$

Анализируя полученные данные методом линейно-кусочной аппроксимации, получаем результаты представленные в таблице 2.

STUDENT	***P***	***A′***	***L***
142 929	66,00	66,00	3
144 280	62,00	62,00	3

195 353	80,00	80,00	4
259 518	62,00	62,00	3
477 284	92,00	92,00	5
502 745	67,00	67,00	3
502 924	75,00	75,00	4
544 181	71,00	71,00	4
544 214	74,00	74,00	4
544 677	74,00	74,00	4
544 792	63,00	63,00	3
…	…	…	…

Таблица 3

где P – оценка за выполнение заданий; A' – уточненный средний балл, L – окончательная оценка, $c_1...c_M$ – вектор граничных значений.

Объективный критерий оценки курса равен:

$$K_{\mathrm{Re}\,z_2} = \frac{L}{\sum_{j=1}^{m} L_j} = 65{,}667 \qquad (1.12)$$

После прохождения теста мы попросили студентов оценить пройденный курс, результаты субъективной оценки и субъективный критерий оценки представлены в таблице 4.

Таблица 4

обратная связь (Ob)	**актуальность материала (Act)**	**наполненность курса (наличие библиотеки) (Nap)**	**колличество времени потраченное на подготовку для данного курса (Kl)**	**являлся ли курс интелектуально сложным (Sl)**	**был ли курс логически связанным (Log)**
2	6	1	2	3	4
1	6	9	9	1	7
4	1	4	7	10	6
3	6	10	1	6	6
2	7	3	5	3	6
9	6	5	5	7	4
3	9	1	10	4	4
10	1	6	4	3	3
1	5	2	8	2	4
4	6	9	6	6	8
9	2	9	2	3	7
8	5	3	8	10	1
4	7	10	2	9	8
2	9	2	9	8	4
…	…	…	…	…	…

Проведя расчёт коэффициентов по каждому критерию получаем результаты представленные в таблице 5.

	Ob	**Act**	**Nap**	**Kl**	**Sl**	**Log**
K_i	50,77	55,20	56,05	55,33	58,47	55,54

При этом коэффициент развития курса: $X_{ij} = \sum \alpha_i k_j = 61.34$, что ниже порогового значения развития курса. Таким образом можем сделать вывод, что данный курс стоит развивать не только по критерию «обратная связь», но и по другим критериям.

Рассмотренные в данной статье метод оценки развития курсов и уровень знаний студентов по изучаемой дисциплине, позволяет предварительно численно оценить качество онлайн курса и наметить пути его улучшения.

Список литературы

1. Юрлова О.А., Колобова О.Л. Дистанционное обучение — актуальная проблема современного образования // Материалы VIII Международной студенческой электронной научной конференции «Студенческий научный форум» URL:<ahref="http://www.scienceforum.ru/2016/1584/25352">www.scienceforum.ru/2016/1584/25352 (дата обращения: 19.12.2017)

2. Артемова О.Г. Проблемы использования дистанционного обучения - Современные образовательные технологии и методы их внедрения в систему обучения: Материалы научно – методической конференции./ Артемова О.Г., Мальцева Н.А.//Вязьма: ВФ ГОУ МГИУ, 2011. – 82с. – ISBN 978–5–902327–77–6.

3. Makarov V.S. Massive open online courses: evaluating the effectiveness and expert advice, Educational Technology, 2014, No 2, P. 38-46.

4. Карпенко М.П. Концепция вуза XXI века // Труды Института государства и права РАН. 2011. №6. URL:http://cyberleninka.ru/article/n/kontseptsiya-vuza-xxi-veka (дата обращения: 15.12.2017).

5. Запорожко В.В., Парфёнов Д.И. Разработка структурной модели массовых открытых онлайн-курсов на базе современных облачных образовательных платформ // Современные наукоемкие технологии. – 2017. – № 3. – С. 12-17; URL:https://top-technologies.ru/ru/article/view?id=36608 (дата обращения: 21.12.2017).

МЕТОДИКИ НАЧАЛЬНОГО ИЗУЧЕНИЯ БЕСПИЛОТНОГО МОБИЛЬНОГО ОБЪЕКТА КАК ОБЪЕКТА ИНФОРМАТИЗАЦИИ В УСЛОВИЯХ КАФЕДРЫ ВУЗА

Аралбаев Т. З., д-р техн. наук, профессор,
Галимов Р. Р., канд. техн. наук, Абрамова Т. В., Каменева Е. В., Халин Г. А.
Оренбургский государственный университет

Под мобильным объектом информатизации (МОИ) в работе понимаются средства и системы обработки информации, используемые в соответствии с заданной информационной технологией, оснащенные системой глобального позиционирования, которые при эксплуатации меняют координаты своего местоположения [4]. Одним из характерных представителей МОИ в настоящее время является класс беспилотных мобильных объектов (БМО), называемых дронами. Популярность и доступность дронов стремительно растёт. За последние пять лет их рынок увеличился в семь раз в мире и в десять раз в России [9]. Это обусловлено широкими возможностями дронов применительно к различным областям деятельности и досуга человека и нашло свое отражение в различных информационных источниках, посвященных производству дронов, их освоению и изучению [2,3,7]. Применение дронов обусловило целый ряд задач, среди которых наиболее актуальными являются задачи защиты от дронов [9] и задачи защиты дронов [1,5,6,8]. Данная работа посвящена разработке начальных принципов освоения дронов, как предметов защиты, в условиях кафедры вуза. Следует отметить, что наряду с большим количеством публикаций по данной тематике, вопросы разработки прикладных методик, учитывающих специфику конкретных условий изучения, доступных инструментальных средств лабораторного типа в литературе освещены недостаточно.

Цель разработки методик: повышение эффективности изучения БМО как объектов защиты в условиях кафедры вычислительной техники и защиты информации Оренбургского государственного университета.

Для достижения цели в процессе исследований разработан комплекс методик, среди которых:

- методика мониторинга за поведением БМО с использованием канала удаленного видеонаблюдения;
- методика мониторинга за поведением БМО на основе захвата и анализа сетевого трафика канала связи.

В качестве БМО использовался квадрокоптер типа Parrot Bebop 2 [10].

В основу первой методики положен принцип дистанционного мониторинга за поведением БМО с использованием удаленного видеонаблюдения. Актуальность данной разработки определена необходимостью предоставления полной информации в учебную аудиторию в условиях дистанционного изучения объекта.

Структурная схема экспериментальной сети дистанционного видеонаблюдения за поведением БМО представлена на рисунке 1.

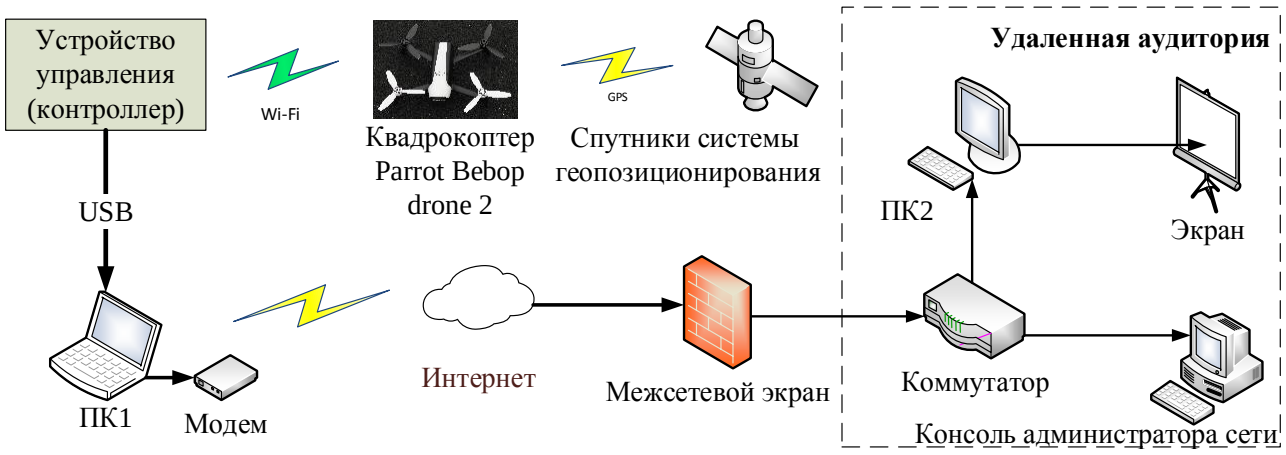


Рисунок 1 – Структурная схема системы удаленного видеонаблюдения за мобильным беспилотным объектом

Данная система позволяет транслировать видеосигнал квадрокоптера из специализированной лаборатории кафедры в одну из удаленных лекционных аудиторий, находящуюся в другом корпусе университета. Изображение, получаемое камерой квадрокоптера, передается с пульта управления квадрокоптером, находящегося в лаборатории кафедры, на настенный экран лекционной аудитории по сети Интернет. Передача информации на экран в лекционной аудитории осуществляется при помощи двух персональных компьютеров (ПК1 и ПК2 на рисунке 2) с предустановленной программой, обеспечивающей голосовую и видеосвязь.

Для реализации связи использованы следующие технические средства:

1. Ноутбук с Wi-Fi адаптером с предустановленной ОС Windows 10;
2. Смартфон с Android OS с предустановленной программой управления дроном.
3. Квадрокоптер Parrot Bebop 2.

Используемое программное обеспечение включает в себя:

1. Freeflight Pro - мобильное приложение для управления дроном.
2. MyPhoneExplorer - программа для синхронизации данных между смартфоном и ПК через USB интерфейс.
3. Skype - программное обеспечение для удаленной видеотрансляции через Интернет.

В целях соблюдения техники безопасности производился контроль отсутствия людей, не связанных с проведением эксперимента, в лабораторных помещениях кафедры.

На рисунке 2 представлено экранное видеоизображение объекта, передаваемое квадрокоптером в лекционную аудиторию в режиме реального времени.

Рисунок 2 – Экранное видеоизображение от объекта

Этот режим позволяет в условиях учебного процесса дистанционно регистрировать видеоданные от квадрокоптера, визуально наблюдать за его поведением в различных режимах и удаленно фиксировать основные характеристики полета: скорость, высоту, уровень сигнала wi-fi и GPS, уровень заряда батареи, положение относительно объектов в помещении.

Вторая методика, в отличие от предыдущей, позволяет изучить поведение БМО на основе «скрытых от глаз» данных сетевого обмена между квадрокоптером и пультом управления с использованием серийных и разработанных аппаратно-программных средств.

Эта методика предназначена для исследования и изучения поведения БМО на основе перехваченного сетевого трафика.

Для перехвата сетевого трафика передаваемого между устройством управления и БМО использовалась утилита Packet Capture из пакета Network Manager [11]. Данный инструмент позволяет перехватывать трафик и сохранять его в файл формата pcap. На этапе исследования данный инструмент устанавливался на устройстве управления. На рисунке 3 представлены результаты перехвата сетевого трафика, полученные при следующих условиях:

- беспилотный мобильный объект имеет IP-адрес 192.168.42.1;
- смартфон, используемый как пульт управления, имеет IP-адрес 192.168.42.33.

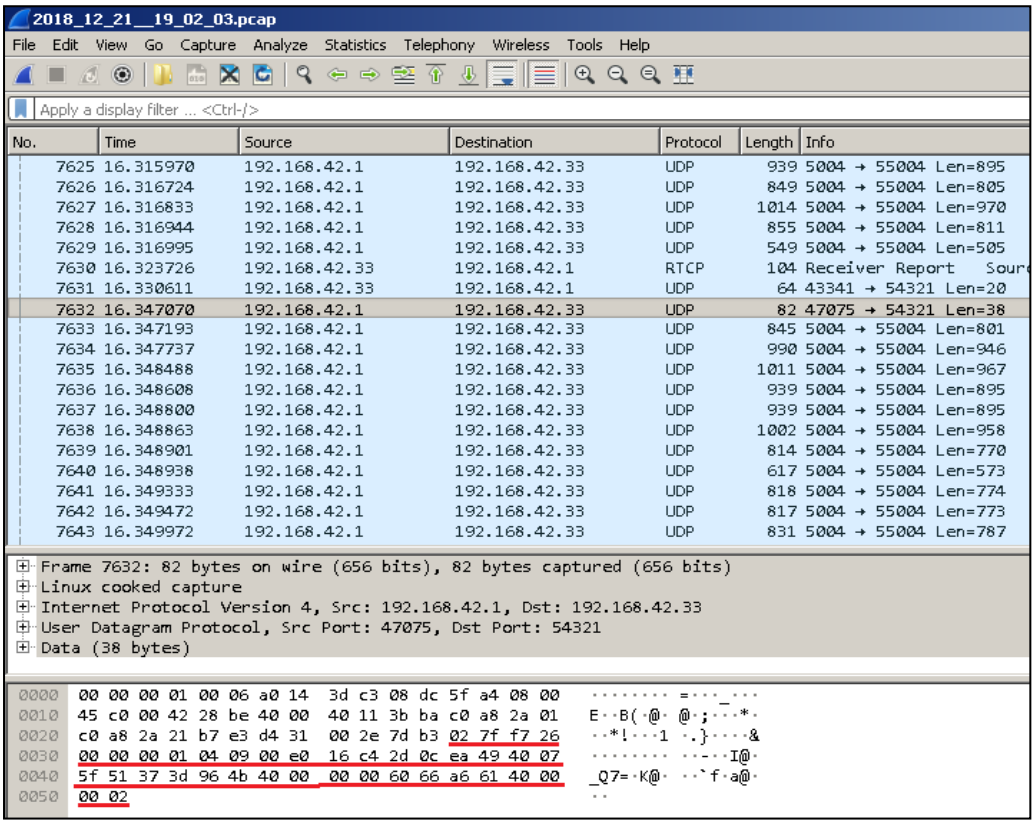


Рисунок 3 – Данные сетевого трафика БМО

В зависимости от этапа взаимодействия с устройством Bebop2 выделяются три типа используемых протоколов:

- на этапе поиска и обнаружения БМО применяется протокол mDNS, который позволяет определить IP-адрес и сервисный порт квадрокоптера;

- этап соединения. В данном режиме используется протокол TCP с ранее определенным сервисным портом. По каналу передается информация в виде строки формата JSON, использующая для определения параметров протокола UDP в основном режиме работы;

- основной режим работы. На данном этапе БМО Bebop2 использует протокол UDP для передачи команд управления и данных, в том числе видеоданных. Описание протокола на прикладном уровне представлено в документе ARSDK Protocols [12].

В рамках данной работы основное внимание уделено протоколу третьего класса. Протокол прикладного уровня квадрокоптера состоит из двух частей: заголовка и непосредственно данных. Заголовок определяет функциональное назначение данного кадра и состоит из 4 полей:

- типа данных (1 байт);
- идентификатор буфера назначения (1 байт);
- порядковый номер обращения к буферу;
- размер всего кадра.

При этом поддерживается 4 типа данных:

- ACK(1) для подтверждения ранее полученных данных;
- Data (2) для передачи обычных данных без подтверждения;

- Low latency data(3) для передачи данных с высоки приоритетом;

- Data with Ack(4) для передачи данных с требованием подтверждения. На рисунке 3 видно, что первый байт в области данных UDP-пакета равен **02h** и определяет передачу обычных данных.

Фактически при передаче данных по сети протокол осуществляет запись в буфер, который можно рассматривать как память типа FIFO, копия которой находится у получателя пакета. При этом каждый класс имеет различные характеристики: по размеру буфера и временным параметрам. С каждым буфером связан счетчик, который увеличивается при каждой передаче данных и используется для выявления повторных пакетов.

В области непосредственных данных кодируются команды или данные. Тип передаваемой информации определяется типом используемого буфера. Например, буфер с идентификатором 127 используется для передачи команд класса ARCommands от дрона к устройству управления.

Команда класса ARCommands, в свою очередь, имеет следующую структуру:

- идентификатор проекта (1 байт);
- идентификатор класса команд (1 байт);
- идентификатор непосредственно команды (2 байта).

Необходимо учитывать, что стек протоколов ARSDK используется для различных типов устройств. Поэтому идентификатор проекта используется для определения набора команд конкретного устройства. Для БМО Bebop2 идентификатор проекта равен 1 и имеет имя «adrone3».

Все команды разделены на группы по функциональному назначению. Например, класс команд «Pilotingstate» с идентификатором «4» содержит следующие команды:

- Flat trim changed (id=0);
- Flying state(id=1);
- Alert state (id=2);
- GpsLocationChanged (id=9).

Далее следуют аргументы команды. Каждая команда характеризуется индивидуальным набором аргументов, которые отличаются как по количеству, так и по типу закодированной информации.

Ниже приведены аргументы команды GpsLocationChanged (изменение навигационных координат):

- широта (double), градусы;
- долгота (double), градусы;
-высота (double), метры;
- погрешность определения широты (uint8);
- погрешность определения долготы (uint8);
- погрешность определения высоты (uint8).

Подробную информацию о командах ARCommands для устройства Bebop2 можно узнать из документа adrone3.xml[13].

Пример декодирования UDP-пакета под номером 7632 (рисунок 3) представлен в таблице 1.

Таблица 1 – Результаты декодирования команды

Значение, hex	Значение, dec	Назначение	Текущее значение
Заголовок прикладного протокола квадрокоптера			
02	2	тип данных	передаются данные без подтверждения
7F	127	тип буфера	передаются данные в формате ARCommands от дрона к пульту управления
F7	247	номер последовательности	идентификатор кадра, переданного по данному буферу
26 00 00 00	38	размер кадра (данные представлены в обратном направлении)	38 байт
ARCommands			
01	1	Идентификатор проекта	Adrone3
04	4	Идентификатор группы команд	Pilotingstate
09 00	9	Идентификатор команды	PositionChanged
Аргументы			
E0-16-C4-2D-0C-EA-49-40	51,828497	Широта(тип double)	51,8284966666668
07-5F-51-37-3D-96-4B-40	55,173743	Долгота (тип double)	55,173743166668
00-00-00-60-66-A6-61-40	141,199997	Высота (тип double)	141,199996948242
00	0	погрешность определения широты (м.)	0
00	0	погрешность определения долготы (м.)	0
02	2	Погрешность определения высоты (м.)	2

Для автоматизации декодирования и изучения сетевых пакетов разработана программа DecodeDronePackets, которая обрабатывает файл с перехваченным сетевым трафиком.

На рисунке 4 представлена экранная форма программы и сохраненные результаты в текстовый файл.

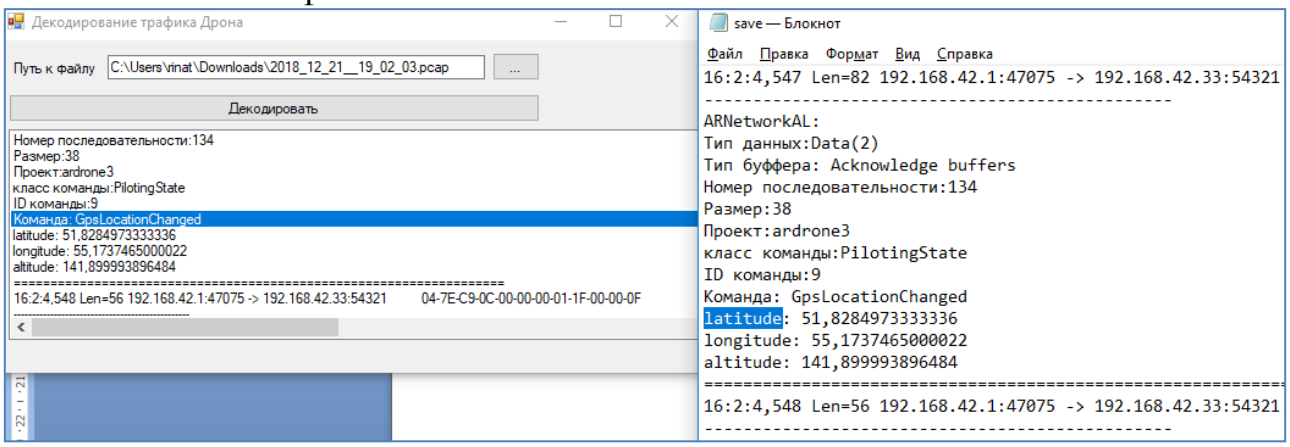


Рисунок 4 – Экранная форма программы декодирования пакетов сетевого трафика квадрокоптера

Результаты данной методики позволяют изучить сетевые протоколы обмена информацией с БМО, наблюдать в режиме реального времени за маршрутом его движения по навигационным данным, а также могут использоваться для обнаружения сетевых атак на подсистему контроля и управления объектом.

Несомненным достоинством предложенных методик является выполнение требований безопасности при работе с мобильными объектами, получение возможности мониторинга объектов по доступной информации, извлекаемой из сетевых каналов связи.

Представленные методики апробированы в учебном процессе кафедры при изучении дисциплин, связанных с проектированием систем защиты мобильных объектов информатизации и исследованием сетевых информационных потоков.

Список литературы

1. Актуальные вопросы обеспечения кибербезопасности беспилотных летательных аппаратов // Военное обозрение [Электронный ресурс]. – URL: http://militaryreview.ru/aktualnye-voprosy-obespecheniya-iberbezopasnosti-bespilotnyx-letatelnyx-apparatov.html - (дата обращения 25.12.2018).

2. Аралбаев, Т. З. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография / Т. З. Аралбаев, Г. Г. Аралбаева, Т. В. Абрамова, Р. Р. Галимов, А. В. Манжосов; Оренбургский гос. ун-т. - Оренбург: ОГУ, 2018. ISBN – 978-5-7410-2202-3

3. Дополнительная общеразвивающая программа «Оператор беспилотных авиационных систем» [Электронный ресурс]. – URL: http://kvant86.ru - (дата обращения 25.12.2018).

4. Каменева, Е. В. Классификация мобильных объектов информатизации / Е. В. Каменева // Теоретические и прикладные вопросы комплексной безопасности:

материалы I Междунар. науч.-практ. конф., 28 марта 2018 г., Санкт-Петербург / Петровская акад. наук и искусств. - Электрон. дан. - Санкт-Петербург: Петровская академия наук и искусств.,2018. - . - С. 170-173.

5. Мухортов, В. В. Защита беспилотных летательных аппаратов от внешних программно-аппаратных воздействий/ В. В. Мухортов, И. Д. Королев// Наука вчера, сегодня, завтра: сб. ст. по матер. XXXII междунар. науч.-практ. конф. № 3(25). – Новосибирск: СибАК, 2016. – С. 87-95.

6. Модель угроз для беспилотника // Бизнес без опасности [Электронный ресурс]. – URL: https://lukatsky.blogspot.com/2015/07/blog-post_21.html - (дата обращения 25.12.2018).

7. Павловский, В. Е. Моделирование и исследование процессов управления квадрокоптером / В. Е. Павловский, С. Ф. Яцун, О. В. Емельянова, А. В. Савицкий //Робототехника и техническая кибернетика. — 2014. — № 4. — С. 49–57.

8. Перечень угроз // ФСТЭК [Электронный ресурс]. – URL: http://bdu.fstec.ru/threat?size=100 - (дата обращения 25.12.2018).

9. «СТОПДРОН» - Защита от беспилотных летательных аппаратов [Электронный ресурс]. - URL: http://stopdron.ru - (дата обращения 25.12.2018).

10. Drone Parrot Bebop 2: обзор модели от французского производителя/ Екатерина // DronGeek. Все о квадрокоптерах и дронах [Электронный ресурс]. - URL: https://drongeek.ru/obzory/parrot/bebop-2 - (дата обращения 25.12.2018).

11. Network Manager - Network Tools & Utilities [Электронный ресурс]. - URL: http://4pda.ru/forum/index.php?showtopic=931360 - (дата обращения 25.12.2018).

12. ARSDK Protocols [Электронный ресурс]. - URL: https://developer.parrot.com/docs/bebop/ARSDK_Protocols.pdf - (дата обращения 25.12.2018).

13. Arsdk-xml [Электронный ресурс]. - URL: https://github.com/Parrot-Developers/arsdk-xml/blob/master/xml/ardrone3.xml - (дата обращения 25.12.2018).

ПРИМЕНЕНИЕ МАКРОСОВ ТАБЛИЧНОГО ПРОЦЕССОРА В ЗАДАЧЕ ИЗУЧЕНИЯ ИМИТАЦИОННОЙ МОДЕЛИ МОНИТОРИНГА ПЕРЕМЕЩЕНИЯ МОБИЛЬНОГО ОБЪЕКТА В ТРЕХМЕРНОМ ПРОСТРАНСТВЕ

Аралбаев Т. З., д-р техн. наук, профессор,
Галимов Р. Р., канд. техн. наук,
Каменева Е. В., Абрамова Т. В., Захаров Е. Ю.
Оренбургский государственный университет

Актуальность темы работы определяется необходимостью подготовки и предоставления методического материала студентам, изучающим вопросы защиты мобильных объектов (МО) информатизации на базе доступных и иллюстративных средств вычислительной техники. В качестве МО в работе использован квадрокоптер типа Drone Parrot Bebop 2 [5].

Анализ методических разработок по теме исследования, в частности, [1,2,4], показал, что в настоящее время перечень работ, позволяющих предоставить учащимся в доступной форме в краткие сроки актуальные сведения по вопросам имитационного моделирования перемещения мобильных объектов в трехмерном пространстве с учетом погрешностей навигационной аппаратуры, ограничен.

Цель работы: освоить методику изучения имитационной модели мониторинга перемещения мобильного объекта с использованием макросов табличного процессора.

Для достижения цели в работе представлены: графическое и математическое описания процесса мониторинга МО, порядок построения имитационной модели с использованием макросов табличного процессора, алгоритм изучения имитационной модели и экранная форма полученных результатов.

Графическая модель трехмерного пространства перемещения МО с указанием зон неопределенности, обусловленных погрешностями навигационной аппаратуры, представлена на рисунке 1. Область перемещения МО представлена в виде вложенных параллелепипедов, границы каждого из которых определяют зоны нормального перемещения МО (S1), допустимого перемещения (S2) и критического перемещения (S3). Границы зон, определены координатами: z1 - z6, находящимися в зонах неопределенности, выделенных прямоугольниками, обусловленными погрешностью навигационной аппаратуры. При получении координат, попадаемых в зоны z в соответствии с допущениями в моделировании, считается, что МО с одинаковой вероятностью может находиться в любой из граничных зон. Следует отметить, что в зависимости от используемой аппаратуры и условий мониторинга погрешность измерения координат может находиться в диапазоне от нескольких сантиметров до нескольких десятков метров.

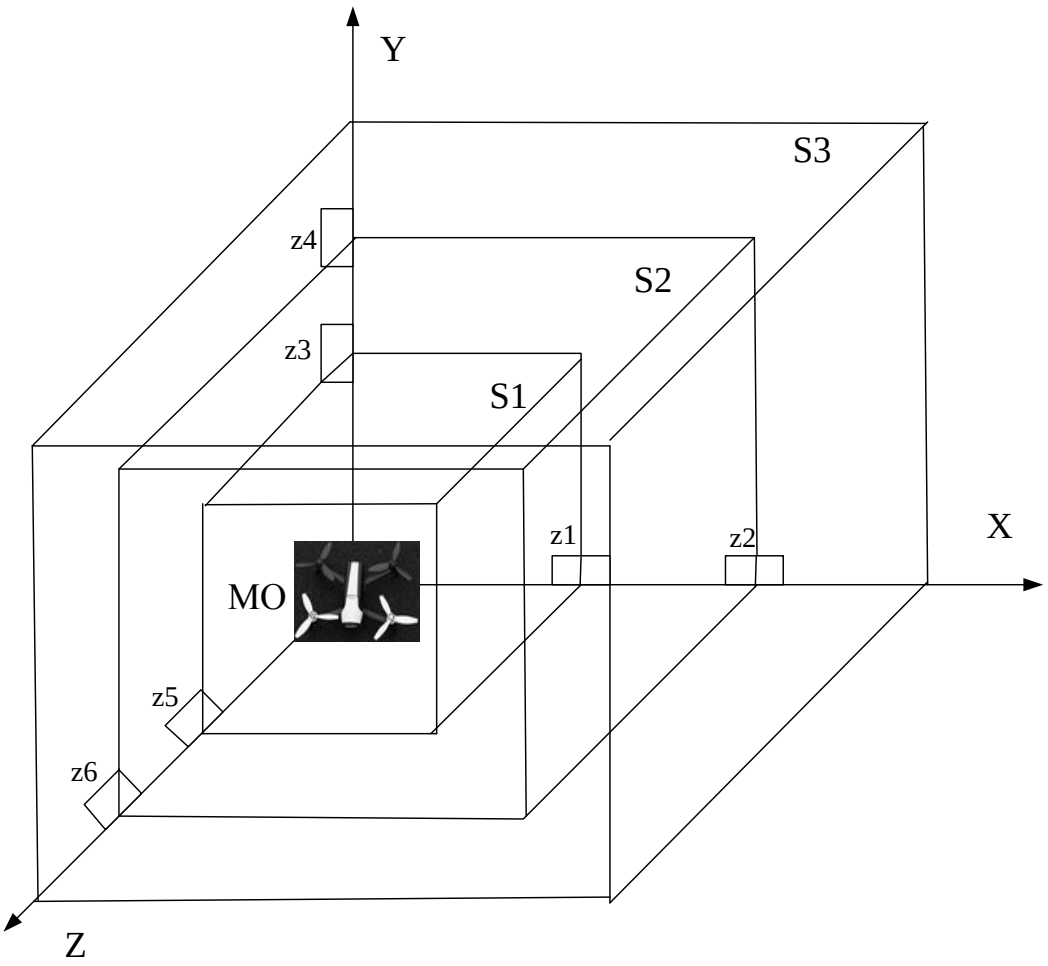


Рисунок 1 – Трехмерная графическая модель пространства перемещения мобильного объекта

Для описания задачи идентификации зоны МО при построении математической модели использованы следующие условные обозначения [1]:

– $S=\{S_1, S_2, S_3\}$ – множество контролируемых зон МО;

– q^x – неизвестный образ зоны, подлежащий распознаванию;

– S^* –образ зоны, к которому отнесен q^x;

– $P = \{X,Y,Z\}$ – множество признаков распознавания образов;

– $<p_i>$ – зарегистрированное значение i-го признака, $i = 1, 3$;

– $<P^x>$ – вектор зарегистрированных значений признаков q^x;

– $D=\{DX_1,DY,DZ\}$ – множество диапазонов изменения признаков, состоящее из множеств поддиапазонов признаков для каждого образа;

– $V\{q^x, S_j\}$ – мера близости между q^x и j-ым образом из множества S, $j= 1, 3$;

– $v_{ij}\{<p_i>, S_j\}$ – частный параметр (коэффициент) ассоциативности значения $<p_i>$ признака p_i из множества P^x для образа S_j;

– $\Phi\{<P^x>, S_j\}$ – разделяющая функция для вычисления меры близости $V\{q^x,P_j\}$;

– $W_j\{<P^x>, D_j\}$ – вектор коэффициентов оценок ассоциативности, характеризующих состояние принадлежности зарегистрированных значений q^x диапазонам значений признаков j-го образа из множества S, $j = 1, 3$;

Модель распознавания q^x имеет следующий вид:

$$V\{q^x, S_j\} = \Phi\{< P^x >, S_j\},\ j = 1,3; \tag{1}$$

$$\Phi\{< P^x >, S_j\} = \sum_{i=1}^{M} v_{ij}\{< p_i{}^x >, S_j\}, i = 1,3; \tag{2}$$

$$v_{ij}\{< p_i{}^x >, S_j\} = \begin{cases} 1, & \text{если} \quad < p_i{}^x > \in D_{ij}; \\ 0, & \text{если} \quad < s_i{}^x > \notin D_{ij}; \end{cases} \tag{3}$$

$$q^x \in S^* \in S : V\{q^x, S^*\} \equiv \max V\{q^x, S_j\}, S_j \in S. \tag{4}$$

Выражение (4) представляет собой правило отнесения q^x к одному из образов множества S по принципу простого большинства с использованием меры Хемминга, либо по принципу превышения суммы ассоциаций более половины признаков.

В зависимости от данных навигационной аппаратуры и принятой системы кодирования состояний положение МО может быть описано кодовыми сигнатурами, представленными в таблице 1. В таблице 1 темным цветом выделены коды несуществующих состояний положения мобильного объекта.

Таблица 1 – Таблица кодов состояний положения мобильного объекта

№ п.п.	X			Y			Z		
	S1	S2	S3	S1	S2	S3	S1	S2	S3
1	0	0	0	0	0	0	0	0	0
2	A			A			A		
	0	0	1	0	0	1	0	0	1
3	B			B			B		
	0	1	0	0	1	0	0	1	0
4	C			C			C		
	0	1	1	0	1	1	0	1	1
5	D			D			D		
	1	0	0	1	0	0	1	0	0
6	1	0	1	1	0	1	1	0	1
7	E			E			E		
	1	1	0	1	1	0	1	1	0
8	1	1	1	1	1	1	1	1	1

В таблице 2 представлены характеристики некоторых сигнатур положения МО.

Таблица 2 – Таблица соответствия кодов и положения мобильного объекта

№ п. п.	Совокупные коды координат			Положение мобильного объекта
1	**A**	**A**	**A**	**Критическое положение МО по координатам X,Y,Z**
2	**A**	**A**	**B**	**Критическое положение МО по координатам X,Y, а по Z – в допустимой зоне**
3	**B**	**B**	**B**	**Допустимое (граничное) положение МО по всем координатам**
4	**A**	**A**	**E**	**Критическое положение МО по координатам X,Y, а по Z в нормально-допустимой зоне**
5	**C**	**C**	**C**	**Положение МО по всем координатам в допустимо-критической зоне**
6	**B**	**C**	**E**	**Положение МО по всем координате Z в допустимо-критической зоне**
7	**D**	**D**	**D**	**Положение МО по всем координате в нормальной зоне**
8	**E**	**E**	**D**	**Положение МО по всем координатам X и Y в нормально допустимой зоне**
9	**E**	**E**	**E**	**Положение МО по всем координатам в допустимой зоне**

Порядок построения имитационной модели с использованием макросов табличного процессора представлен на экранной форме имитационной модели (рисунок 2) и имеет ниже перечисленные пункты.

1. Задаются различными цветами области диапазонов координат перемещения МО.

2. С использованием генератора случайных чисел задаются координаты по осям X,Y, и Z.

3. В соответствии с математическими выражениями программируется таблица 1 для идентификации состояния $\boldsymbol{S}^{*}$.

4. С применением макросов табличного процессора программируются таблицы 2 и 3. представленные на рисунке 2, для исследования динамики перемещения МО.

5. Программируются процедуры вывода результатной информации в виде графиков перемещения МО по зонам: S1, S2 и S3.

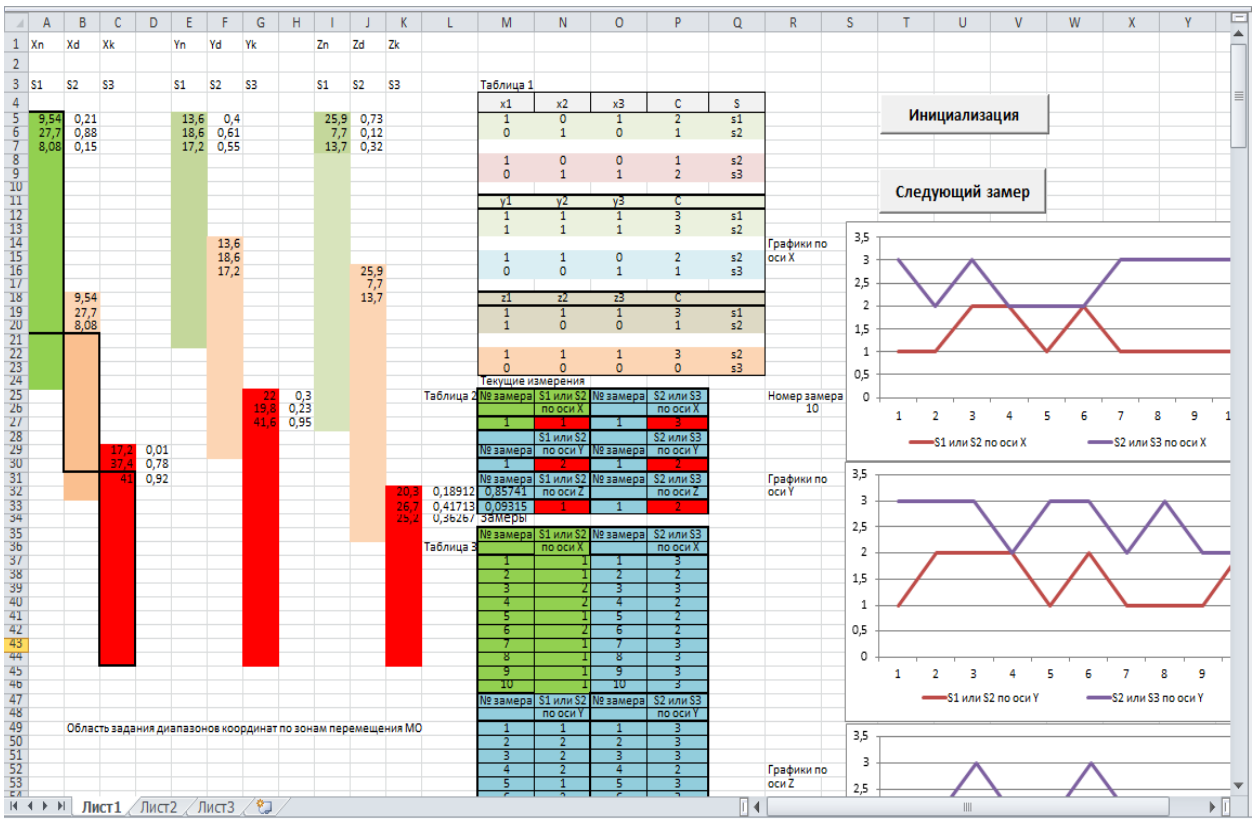


Рисунок 2 – Экранная форма процесса имитационного моделирования перемещения МО в трехмерном пространстве с использованием макросов табличного процессора

Разработанная в табличном процессоре Excel имитационная модель на основе формул обычно позволяет получить результаты для текущих данных для одного шага некоторого процесса. Для исследования модели в динамике для ряда последовательных тактов применение только данного механизма является недостаточным, поскольку необходимо сохранять данные предыдущего цикла, задавать текущие данные для каждого нового шага, каждый раз запускать программу и выводить непрерывно и последовательно все результаты в виде одного графика.

Одним из решений задачи устранения этого недостатка является использование макросов, созданных при помощи языка Visual Basic Application (VBA) [3]. В рамках данной работы разработаны макросы Init и Next, вызываемые по нажатию кнопок «Инициализация» и «Следующий замер», соответственно. По нажатию первой кнопки вызывается макрос, сохраняющий предыдущие результаты исследования и подготавливающий пространство в окне программы для следующего шага. Вторая кнопка увеличивается счетчик номера замера, обновляет входные данные модели при помощи генератора случайных чисел и сохраняет рассчитанные данные при помощи формул в позиции таблицы 3, соответствующие номеру эксперимента. При этом результат идентификации положения МО отражается на графиках, на которых регистрируется состояние МО для каждой текущей координаты. На рисунке 3 представлена экранная форма

программного кода макроса Next.

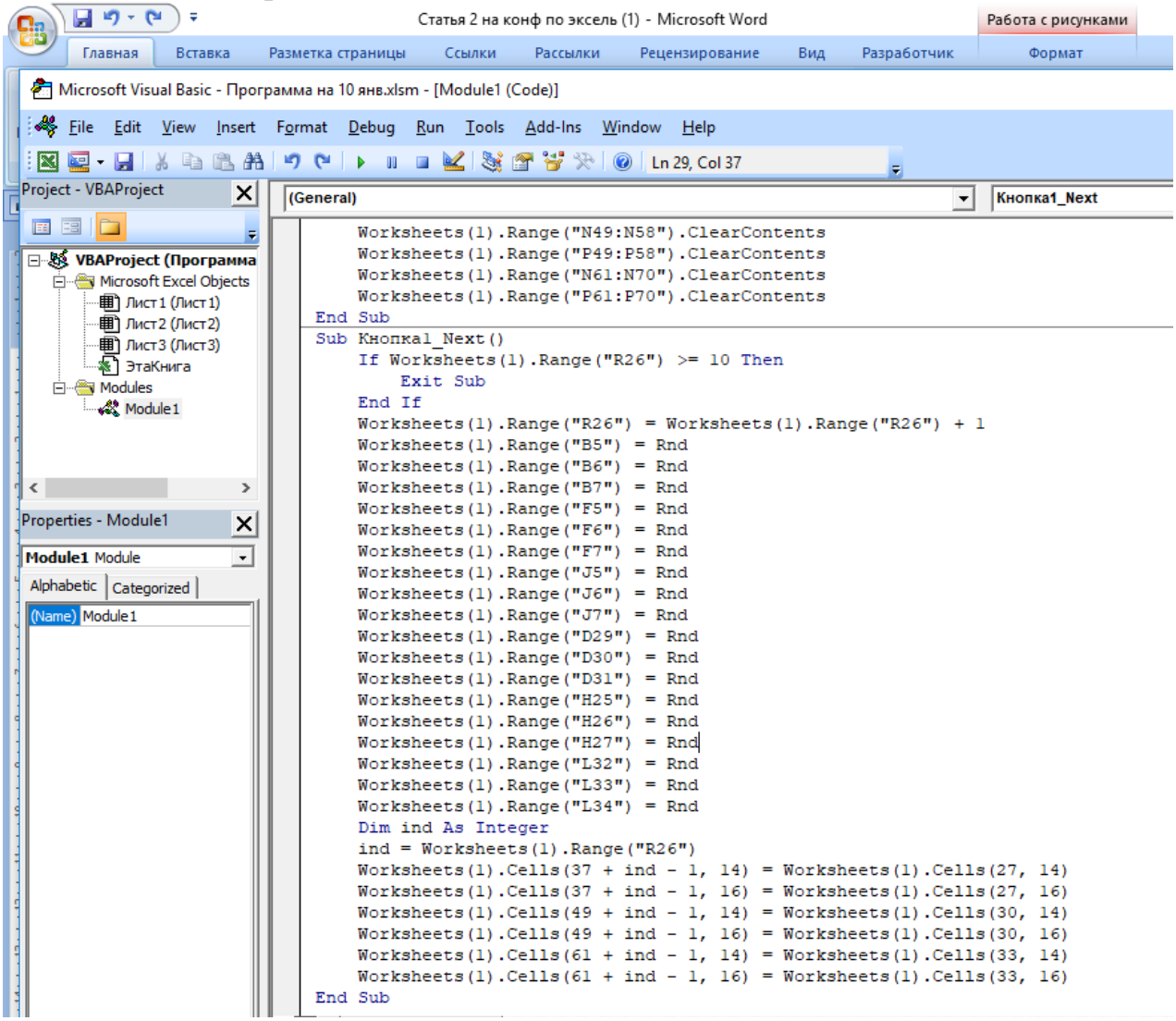


Рисунок 3 – Экранная форма программного кода макроса

Таким образом, использование макросов позволяет автоматизировать процесс проведения вычислительных экспериментов и исследовать модель в динамике. При этом необходимо отметить простоту программирования, использования и реализации макросов.

Достоинства предложенной методики:

- доступность и наглядность представления относительно сложного материала, такого как имитационное моделирование, средствами приложений к операционной системе компьютера;
- многовариантность постановок задач исследований на базе одного оконного интерфейса;
- возможность использования имитационной программы студентами с различным уровнем подготовки в области знаний языков программирования;

- рассмотренная программа может быть интегрирована с программами на языках высокого уровня для демонстрации и визуализации результатов моделирования.

Данная методика успешно апробирована в процессе выполнения лабораторных работ, работ по курсовому и дипломному проектированию по дисциплинам бакалавриата и магистратуры студентами профиля «Комплексная защита объектов информатизации» и магистерской программы по направлению «Информатика и вычислительная техника» на кафедре вычислительной техники и защиты информации ОГУ.

Список литературы

1. Аралбаев, Т. З. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография / Т. З. Аралбаев, Г. Г. Аралбаева, Т. В. Абрамова, Р. Р. Галимов, А. В. Манжосов; Оренбургский гос. ун-т. - Оренбург: ОГУ, 2018. -160 с. ISBN – 978-5-7410-2202-3

2. Дополнительная общеразвивающая программа «Оператор беспилотных авиационных систем» [Электронный ресурс]. – URL: http://kvant86.ru - (дата обращения 25.12.2018).

3. Михеев Р.Н. VBA и программирование в MS Office для пользователей/ Р.Н. Михеев. –СПб.: БХВ-Петербург, 2006. -384 с.

4. Павловский, В. Е. Моделирование и исследование процессов управления квадрокоптером / В. Е. Павловский, С. Ф. Яцун, О. В. Емельянова, А. В. Савицкий //Робототехника и техническая кибернетика. — 2014. — № 4. — С. 49–57.

5. Drone Parrot Bebop 2: обзор модели от французского производителя/ Екатерина // DronGeek. Все о квадрокоптерах и дронах [Электронный ресурс]. - URL: https://drongeek.ru/obzory/parrot/bebop-2 - (дата обращения 25.12.2018).

ПРИМЕНЕНИЕ ПАКЕТА NIST STS ДЛЯ РЕШЕНИЯ УЧЕБНЫХ ЗАДАЧ ДИСЦИПЛИНЫ «ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ»

Благовисная А.Н., Самойлов Е.И.*, Давлетбаев А.Ф.
Оренбургский государственный университет, ООО «Комдиагностика»*

Одной из задач освоения дисциплины «Теория псевдослучайных генераторов» является приобретение навыков решения задач оценки качества генераторов псевдослучайных последовательностей [1]. Оценить качество генераторов псевдослучайных последовательностей с точки зрения случайности позволяют статистические тесты, использующие методы статистического анализа для определения близости генерируемой последовательности к истинно случайной.

Изучение методов тестирования последовательностей предусматривает решение учебных задач, заключающихся в применении алгоритмов тестирования последовательностей и анализе результатов. Практика преподавания дисциплин, в которых изучаются методы защиты информации, показала, что на первоначальном этапе знакомства с технологиями тестирования псевдослучайных последовательностей необходимо иметь программный инструментарий, позволяющий проводить анализ результатов тестирования.

Статистические тесты обычно объединяются в пакеты, представляющие собой подборку различных статистических методик по оценке качества псевдослучайных последовательностей. Наиболее распространенными и известными являются пакеты Diehard, TestU01, NIST, CRYPT-X, тесты Д. Кнута. В работе [2] нами проанализированы достоинства и недостатки пакетов тестов Diehard, TestU01, NIST STS. Установлено преимущество пакета NIST как наиболее разработанного стандарта, предназначенного для сертификации генераторов псевдослучайных последовательностей и отвечающего различным областям применения псевдослучайных чисел. Именно NIST STS выбран нами и реализован для проведения учебных занятий по исследованию генераторов псевдослучайных последовательностей. В работе [3] описано программное средство, реализующее статистический пакет NIST. Отличительной особенностью данной реализации является ориентированность программного средства на пользователя. Дружественный, интуитивно понятный интерфейс позволяет использовать программу в учебном процессе.

Продемонстрируем применение статистического пакета NIST для решения учебных задач диципины «Теория псевдослучайных генераторов» на примере исследования фильтрующих и комбинирующих генераторов.

Формулировка задания. Реализовать фильтрующие и комбинирующие генераторы. Исследовать характеристики фильтрующих и комбинирующих генераторов, вырабатывающих последовательности, в зависимости от прохождения статистических тестов.

Для выполнения задания сначала необходимо реализовать фильтрующие и комбинирующие генераторы, затем получить последовательности,

вырабатываемые генераторами с различными характеристиками, исследовать полученные последовательности с помощью пакета NIST, а затем сделать выводы о прохождении статистических тестов в зависимости от харакеристик генераторов.

Фильтрующие и комбинирующие генераторы являются структурными компонентами некоторых классических поточных шифров [4]. Они строятся на основе линейных регистров сдвига и булевой функции f, которая является функцией усложнения.

Схема фильтрующего генератора представлена на рисунке 1. На вход регистра сдвига подаётся последовательность, являющаяся ключом для криптосистемы. На выходе из регистра сдвига последовательность поступает в фильтр, где усложняется булевой функцией.

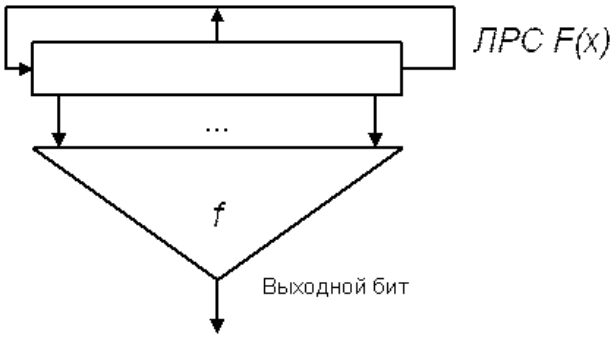


Рисунок 1 – Схема фильтрующего генератора

Схема комбинирующего генератора представлена на рисунке 2. Комбинирующие генераторы можно рассматривать как усложнение фильтрующих генераторов. На вход усложняющей булевой функции поступают элементы линейных рекуррентных последовательностей, вырабатываемые линейными регистрами.

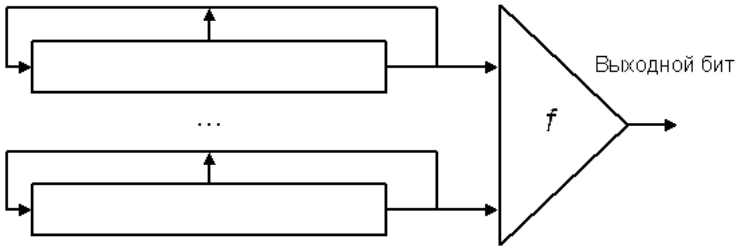


Рисунок 2 – Схема комбинирующего генератора

Работу линейных регистров сдвига можно описать линейными рекуррентными уравнениями вида:

$$\forall i \in \square_0 : u(i+m) = c_{m-1}u(i+m-1) \oplus ... \oplus c_1 u(i+1) \oplus c_0 u(i), \text{ где } c_0, c_1, ...c_{m-1} \in F_2 .$$

С линейным рекуррентным уравнением можно связать многочлен $F(x) = x^n \oplus c_{m-1}x^{n-1} \oplus ... \oplus c_1 x \oplus c_0$ над полем F_2, называемый характеристическим многочленом линейной рекуррентной последовательности.

В качестве функций усложнения в генераторах используется булева функция. Булевы функции будем представлять в алгебраической нормальной форме [4].

Приведем пример реализованного при выполнении задания программного средства. Интерфейс программного средства представлен на рисунке 3.

При работе с программным средством необходимо выбрать тип генератора, длину генерируемой последовательности, задать типы регистров сдвига и усложняющих булевых функций. Программа реализует как комбинирующий, так и фильтрующий типы генераторов. При выборе комбинирующего генератора можно использовать до трёх регистров сдвига.

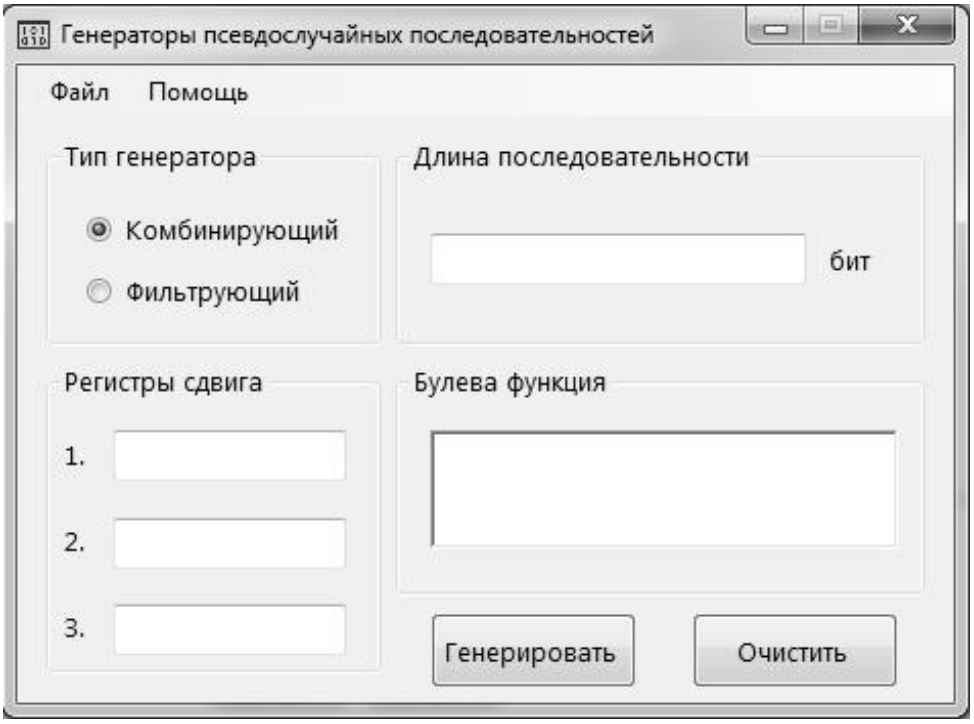


Рисунок 3. Программное средство «Генераторы псевдослучайных последовательностей»

Для обеспечения стойкости к различным видам атак функции усложнения в фильтрующих и комбинирующих генераторах должны удовлетворять ряду требований, к которым относят алгебраическую степень, нелинейность, уравновешенность, устойчивость, корреляционную иммунность, алгебраическую иммунность, отсутствие запрета и т.д. При выполнении задания в качестве функций усложнения необходимо выбирать булевы функции, удовлетворяющие ряду криптографических характеристик. Пусть ключевыми для данного примера характеристиками будут уравновешенность, нелинейность, алгебраическая степень, алгебраическая иммунность.

Функции усложнения применяются к линейным рекуррентным последовательностям, построенным на основе уравнений рекурсии, характеристические многочлены которых являются неприводимыми.

На основе выбранных булевых функций осуществляется усложнение линейной рекуррентной последовательности. Усложнённая последовательность является результатом работы фильтрующего или комбинирующего генератора.

К получившимся в результате работы генераторов последовательностям применяются статистические тесты NIST. Приведем примеры характеристик фильтрующих и комбинирующих генераторов, а также результаты тестирования соответствующих им последовательностей в таблице 1.

Таблица 1 – Примеры характеристик исследуемых генераторов и результаты тестирования соответствующих им последовательностей

Уравнения рекурсии, фильтрующая или комбинирующая булева функция	Значения характеристик булевых функций					Длины последовательностей	Количество пройденных тестов
	Уравновешенность	Алгебраическая степень	Значение нелинейности	Значение алгебраической иммунности	Выполнение строгого лавинного критерия		
$u(i+4)=u(i+2)\oplus u(i)$, $f=x_1x_2x_4\oplus x_1x_2\oplus x_1x_3\oplus x_1x_4\oplus$ $\oplus x_2x_3\oplus x_3x_4\oplus x_1\oplus x_2\oplus x_4\oplus 1$	+	3	4	2	+	100000	3
$u(i+5)=u(i+2)\oplus u(i)$, $f=x_1x_2x_3x_5\oplus x_1x_2x_4x_5\oplus$ $\oplus x_1x_3x_4x_5\oplus x_1x_2x_5\oplus x_1x_4x_5\oplus$ $\oplus x_2x_3x_4\oplus x_2x_3x_5\oplus x_2x_4x_5\oplus$ $\oplus x_1x_3\oplus x_1x_4\oplus x_2x_3\oplus$ $\oplus x_3x_5\oplus x_2\oplus x_4\oplus x_5$	+	4	10	2	–	100000	1
$u(i+8)=u(i+7)\oplus u(i+6)\oplus$ $\oplus u(i+5)\oplus u(i+4)\oplus u(i+1)\oplus u(i)$, $u(i+7)=u(i+6)\oplus u(i+3)\oplus$ $\oplus u(i+1)\oplus u(i)$, $u(i+6)=u(i+5)\oplus u(i+2)\oplus$ $\oplus u(i+1)\oplus u(i)$, $f=x_1x_3\oplus x_1\oplus x_2$	+	2	2	2	–	100000	9
$u(i+15)=u(i+14)\oplus u(i)$, $u(i+14)=u(i+13)\oplus$ $\oplus u(i+12)\oplus u(i+2)\oplus u(i)$, $u(i+13)=u(i+12)\oplus$ $\oplus u(i+11)\oplus u(i+8)\oplus u(i)$, $f=x_2x_3\oplus x_1\oplus x_3\oplus 1$	+	2	2	2	–	100000	10

В процессе анализа результатов тестирования необходимо сформулировать выводы о связи характеристик генераторов и статистических тестов, которые проходят последовательности, вырабатываемые данными генераторами.

В качестве примера рассмотрим выводы, полученные в результате решения рассматриваемой задачи:

– большее количество тестов проходят последовательности, получаемые с помощью комбинирующих генераторов вне зависимости от длины регистров сдвига и характеристик булевых функций;

– последовательности фильтрующих генераторов проходят некоторые из тестов, начиная с длины регистра сдвига, равной 4. Прохождение тестов последовательностями в данном случае больше зависит от длины регистра сдвига, чем от свойств функции усложнения. В основном последовательности проходят частотный побитовый, частотный блочный тесты и тест кумулятивных сумм;

– последовательности комбинирующих генераторов проходят тесты практически для любых сочетаний длин и уравнений рекурсий регистров сдвига. Чем больше длина регистров сдвига, тем больше тестов проходят последовательности. Наибольшее количество тестов проходят те последовательности, у которых функции усложнения являются уравновешенными и удовлетворяют строгому лавинному критерию. Анализ уравнений регистров сдвига показал, что большее количество тестов проходят последовательности, получаемые с помощью генераторов, у которых в регистрах сдвига наблюдаются несколько подряд идущих отводов, обеспечивающих обратную связь.

Список литературы

1. Рабочая программа дисциплины «Б.1.В.ДВ.7.1 Теория псевдослучайных генераторов» / сост. А.Н. Благовисная. – Оренбург: ОГУ, 2018.

2. Самойлов, Е. И. О программных реализациях тестов псевдослучайных последовательностей / Е. И. Самойлов, А. Н. Благовисная // Университетский комплекс как региональный центр образования, науки и культуры [Электронный ресурс]: материалы Всероссийской научно-методической конференции; Оренбург. гос. ун-т. – Оренбург: ОГУ, 2018. – С. 1751-1754.

3. Самойлов, Е.И. Учебное программное средство тестирования псевдослучайных последовательностей / Е. И. Самойлов, А. Н. Благовисная // Вестник современных исследований. – 2018. – № 5-1 (20). – С. 510-513.

4. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – М.: МЦНМО, 2012. – 583 с.

ПРИМЕНЕНИЕ СИСТЕМЫ SAGE ДЛЯ ПОИСКА АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ БУЛЕВЫХ ФУНКЦИЙ И ОТОБРАЖЕНИЙ

Благовисная А.Н., Симуськова И.О.
Оренбургский государственный университет

Булева функция является одним из важнейших математических понятий, исследуемых в современной криптографии. Это обусловлено тем, что булевы функции и отображения используются в качестве структурных элементов множества криптографических конструкций. С помощью булевых функций описываются структурные компоненты блочных, поточных шифров, а также широко известные криптографические хэш-функции. Функции или их системы, применяемые при синтезе криптографических объектов, называются криптографическими функциями. Развитие методов и средств криптографического анализа привело к формулировке ряда требований, предъявляемых к криптографическим функциям. Эти требования получили название криптографических свойств. Булевы функции, удовлетворяющие специальным криптографическим характеристикам, вносят существенный вклад в стойкость криптографических алгоритмов. Исследование криптографических характеристик, методов и алгоритмов создания булевых функций с криптографическими характеристиками являются актуальными задачами современной криптографии.

Основным свойством булевых функций, характеризующим способность шифра противостоять алгебраическим атакам, является алгебраическая иммунность. Существует множество публикаций как отечественных, так и зарубежных авторов, посвященных различным проблемам теории и практики применения криптографических булевых функций. В статьях, монографиях и книгах, в которых рассматриваются вопросы криптографических приложений булевых функций, отражаются следующие направления исследований, связанные с понятием алгебраической иммунности:

– получение оценок и разработка алгоритмов вычисления значения алгебраической иммунности булевых функций;

– исследование оптимальных сочетаний криптографических свойств булевых функций;

– разработка методов и алгоритмов построения криптографических булевых функций с оптимальными сочетаниями свойств, включая алгебраическую иммунность;

– реализация алгебраических атак на криптографические конструкции.

Рассмотрим булеву функцию f от n переменных. Булева функция g от n переменных называется аннигилятором функции f, если $fg=0$.

Алгебраической иммунностью $AI(f)$ булевой функции f называется минимальное число d такое, что существует булева функция g (аннигилятор) степени d, не тождественно равная нулю, для которой выполняется одно из равенств $fg \equiv 0$ или $(f \oplus 1)g \equiv 0$ [6].

Для создания криптографических булевых функций важно уметь находить значение алгебраической иммунности булевой функции.

Известно, что для любой булевой функции от *n* переменных $AI(f) \le \left\lceil \frac{n}{2} \right\rceil$ [6].

В работах [1, 2, 5, 6] описаны алгоритмы, позволяющие получать значения алгебраической иммунности булевых функций.

Продемонстрируем поиск алгебраической иммунности для функции $f(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 \oplus x_2x_3x_4 \oplus x_3x_4$.

Так как $AI(f) \le 2$, то нам достаточно выяснить, существуют ли аннигиляторы g для булевой функции *f*, степень которых $\deg g = 1$. Представим функцию g в виде $g(x_1, x_2, x_3, x_4) = a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_4x_4 \oplus a_0$, где $a_1, a_2, a_3, a_4, a_0 \in F_2$.

По определению

$$fg = (x_1x_2x_3x_4 \oplus x_2x_3x_4 \oplus x_3x_4)(a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_4x_4 \oplus a_0) \equiv 0 \quad (1)$$

или

$$\begin{aligned}&(f \oplus 1)g = \\ &= (x_1x_2x_3x_4 \oplus x_2x_3x_4 \oplus x_3x_4 \oplus 1)(a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_4x_4 \oplus a_0) \equiv 0.\end{aligned} \quad (2)$$

Выясним, при каких a_1, a_2, a_3, a_4, a_0 выполняются данные соотношения.

В левой части равенства (1) раскроем скобки и приведем подобные слагаемые. Получим

$$\begin{aligned}&(a_2 \oplus a_3 \oplus a_4 \oplus a_0)x_1x_2x_3x_4 \oplus (a_3 \oplus a_4 \oplus a_0)x_2x_3x_4 \oplus \\ &\oplus a_1x_1x_3x_4 \oplus (a_3 \oplus a_4 \oplus a_0)x_3x_4 \equiv 0.\end{aligned} \quad (3)$$

Значения a_1, a_2, a_3, a_4, a_0, при которых равенство (3) является верным, найдем из системы уравнений:

$$\begin{cases} a_2 \oplus a_3 \oplus a_4 \oplus a_0 = 0, \\ a_3 \oplus a_4 \oplus a_0 = 0, \\ a_1 = 0, \\ a_3 \oplus a_4 \oplus a_0 = 0. \end{cases} \quad (4)$$

На данном этапе поиска значения алгебраической иммунности достаточно найти хотя бы одно ненулевое решение системы (4) или доказать, что система (4) имеет единственное тривиальное решение.

Система (4) имеет нетривиальные решения. Например, $a_1 = 0$, $a_2 = 0$, $a_3 = 1$, $a_4 = 0$, $a_0 = 1$. Это означает, что существует аннигилятор, степень которого равна 1. Итак, алгебраическая иммунность булевой функции равна 1.

Исследование криптографических булевых функций невозможно без применения программных средств, позволяющих автоматизировать процессы нахождения числовых характеристик булевой функции. К таким программным средствам относят математические пакеты, имеющие широкий спектр возможностей для работы в различных областях математики: Maple, Matlab, REDUCE, MACSYMA, MuPAD и другие. Математические системы данного типа включают в себя большое количество средств работы с различными математическими объектами, в том числе позволяют организовать работу с многочленами и осуществлять поиск решения системы алгебраических уравнений.

Среди математических пакетов существует бесплатное и доступное математическое программное обеспечение, например, система компьютерной алгебры Sage, относящаяся к свободному программному обеспечению, распространяемому по условиям лицензии GNU GeneralPublicLicense. Система Sage позволяет решать задачи из различных областей математики, в том числе решать задачи теории многочленов, заданных над конечными полями [4]. На данный момент нам не удалось найти доступных инструментов пакета Sage, осуществляющих процесс формирования систем булевых уравнений, получающихся в процессе выполнения некоторых этапов алгоритма поиска алгебраической иммунности. Однако решение систем линейных уравнений над конечными полями в пакете Sage осуществить возможно. В качестве примера рассмотрим решение системы булевых уравнений (4).

Так как необходимо решить однородную систему булевых уравнений, то можно задать матрицу системы одним из известных способов задания матриц над конечными полями и привести её к ступенчатому виду:

```
sage: M = MatrixSpace(GF(2),4,5)
sage: A = M([0,1,1,1,1, 0,0,1,1,1, 1,0,0,0,0, 0,0,1,1,1])
sage: A.rref()
```

В результате система Sage выдает ступенчатую матрицу в следующем виде:

```
[1 0 0 0 0]
[0 1 0 0 0]
[0 0 1 1 1]
[0 0 0 0 0]
```

Полученная матрица соответствует системе

$$\begin{cases} a_1 = 0, \\ a_2 = 0, \\ a_3 \oplus a_4 \oplus a_0 = 0, \end{cases}$$

откуда можно найти как общее, так и частное решения.

Другой подход к решению системы булевых уравнений заключается в том, чтобы найти базисные векторы пространства решений:

```
sage: A = matrix(GF(2),[[0,1,1,1,1], [0,0,1,1,1], [1,0,0,0,0], [0,0,1,1,1]])
sage: B = vector(GF(2),[0,0,0,1])
sage: X = A.right_kernel(basis='pivot')
sage: X
```

Результат выполнения данных команд следующий:

```
Vector space of degree 5 and 2 over Finite Field of size 2
User basis matrix:
[0 0 1 1 0]
[0 0 1 0 1]
```

Таким образом, можно сделать вывод о существовании ненулевых решений системы (4) и существовании аннигилятора булевой функции, степень которого равна 1.

При построении нелинейных узлов (S-блоков) блочных симметричных шифров используются криптографические булевы отображения $\Phi : F_2^n \to F_2^m$.

Понятие алгебраической иммунности булевых функций можно обобщить на случай булевых отображений (векторных булевых функций). Более подробную информацию об обобщениях понятия алгебраической иммунности можно найти, например, в [7]. Рассмотрим определение алгебраической иммунности булевых отображений в соответствии с работой [5].

S-блок задается системой алгебраических уравнений над полем F_2:

$$\begin{cases} f_1(x_1, x_2, ..., x_n) = y_1, \\ f_2(x_1, x_2, ..., x_n) = y_2, \\ ... \\ f_m(x_1, x_2, ..., x_n) = y_m. \end{cases} \quad (5)$$

С системой (5) связан идеал, порожденный булевыми многочленами:

$$I(S) = (f_1(x_1, x_2, ..., x_n) \oplus y_1, f_2(x_1, x_2, ..., x_n) \oplus y_2, ..., f_m(x_1, x_2, ..., x_n) \oplus y_m). \quad (6)$$

Алгебраическая иммунность нелинейного узла блочного симметричного шифра $AI(S)$ определяется как минимальная степень многочлена из идеала $I(S)$.

Для вычисления алгебраической иммунности $AI(S)$ необходимо построить минимальный редуцированный базис Грёбнера идеала $I(S)$ системы (5) и среди элементов базиса найти многочлен минимальной степени.

Продемонстрируем поиск алгебраической иммунности булевых отображений, задающих S-блок шифра Baby-Rijndael в системе Sage. Булевы функции и отображения S-блока данного шифра рассмотрены в статье [3]. Согласно восстановленным АНФ для компонентных булевых функций S-блок шифра Baby-Rijndael можно представить в виде следующей системы:

$$\begin{cases} x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_2 \oplus x_4 = y_1, \\ x_1x_2x_3 \oplus x_1x_3x_4 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1 \oplus x_3 \oplus x_4 \oplus 1 = y_2, \\ x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_1x_4 \oplus x_3x_4 \oplus x_1 \oplus x_4 = y_3, \\ x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1 \oplus x_2 \oplus x_4 \oplus 1 = y_4. \end{cases} \quad (7)$$

С этой системой связан следующий идеал:

$$I(S) = (x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_2 \oplus x_4 \oplus y_1,$$
$$x_1x_2x_3 \oplus x_1x_3x_4 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1 \oplus x_3 \oplus x_4 \oplus 1 \oplus y_2,$$
$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2 \oplus x_1x_4 \oplus x_3x_4 \oplus x_1 \oplus x_4 \oplus y_3,$$
$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1 \oplus x_2 \oplus x_4 \oplus 1 \oplus y_4).$$

Для полученного идеала найдем минимальный редуцированный базис Грёбнера в системе Sage.

Сначала задаем кольцо многочленов и идеал $I(S)$ системы (7):

```
sage: P.<x1,x2,x3,x4, y1,y2,y3,y4> = PolynomialRing(GF(2), 8, order = 'degrevlex')
sage: q = P.base_ring().order()
sage: Q = P.quotient_ring(ideal([var**q - var for var in P.gens()]))
sage: f1 = y1+x1*x2*x4+x1*x3*x4+x2*x3*x4+x2*x3+x3*x4+x2+x4
sage: f2 = y2+x1*x2*x3+x1*x3*x4+x1*x2+x2*x4+x3*x4+x1+x3+x4+1
sage: f3 = y3+x1*x2*x3+x1*x2*x4+x1*x2+x1*x4+x3*x4+x1+x4
sage: f4 = y4+x1*x2*x3+x1*x2*x4+x1*x3*x4+x2*x3*x4+ \
                              x1*x3+x1*x4+x2*x4+x1+x2+x4+1
sage: I = (f1,f2,f3,f4)*P
```

Выясняем, образует ли идеал *I* базис Грёбнера:

```
sage: I. basis_is_groebner ()
```

Получаем результат:

False

Таким образом, идеал $I(S)$ системы (7) базисом Грёбнера не является.
Находим базис Грёбнера:

sage: B = I.groebner_basis(); B

В результате получаем сообщение:

Polynomial Sequence with 60 Polynomials in 8 Variables

Изучая все многочлены базиса Грёбнера, находим, что многочленом минимальной степени является многочлен степени 2. Например:

sage: B = I.groebner_basis()
sage: Q(B[56])
*x1bar*x3bar + x2bar*x3bar + x3bar*x4bar + x1bar*y1bar + x4bar*y1bar + x1bar*y2bar + x1bar*y3bar + x4bar*y4bar + x2bar + x3bar + x4bar + y1bar + y2bar +1*

Таким образом, алгебраическая иммунность S-блока, задаваемого системой (7), равна 2.

Заметим, что поиск алгебраической иммунности булевых функций и отображений с помощью средств системы Sage удобен для решения учебных задач, содержащих небольшое количество входных данных и направленных на понимание определений и алгоритмов поиска алгебраической иммунности. Для работы с булевыми функциями криптографических конструкций необходимы программные инструменты, реализующие работу с большими объемами данных и учитывающие специфику кольца булевых функций.

Список литературы

1. Баев, В. В. О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций // Дискретная математика. – 2006. – Т. 18. – № 3. – С. 138-151.

2. Баев, В. В. Усовершенствованный алгоритм поиска аннигиляторов низкой степени для многочлена Жегалкина // Дискретная математика. – 2007. – Т. 19. – № 4. – С. 132-138.

3. Долгов, В.И. Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / В.И. Долгов [и др.] // Прикладная радиоэлектроника. – 2009. – Т. 8. – № 3. – С. 268-277.

4. Голубков А.Ю. Компьютерная алгебра в системе Sage: учебное пособие / А.Ю. Голубков, А.И. Зобнин, О.В. Соколова. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2013. – 79 с.

5. Кузнецов, А. А. Алгебраический иммунитет нелинейных узлов симметричных шифров / А. А. Кузнецов [и др.] // Прикладная радиоэлектроника. – 2016. – № 4 (4). – С. 42-55.

6. Логачёв, О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачёв [и др.]. – М.: МЦНМО, 2012. – 583 с.

7. Покрасенко, Д. П. Об алгебраической иммунности векторных булевых функций / Д. П. Покрасенко // ПДМ. Приложение. – 2015. – № 8. – С. 37–39.

УЧЕБНО-МЕТОДИЧЕСКИЕ ПРИМЕРЫ ПОСТРОЕНИЯ РАДИКАЛОВ КОЛЕЦ

Благовисная А.Н., Горелик А.А.
Оренбургский государственный университет

Понятие радикала алгебраической системы играет важную роль в современной алгебре. Впервые это понятие возникло в исследованиях Ф.Э. Молина, Э. Картана, Дж. Ваддерберна о конечно порожденных ассоциативных алгебрах. Впоследствии появились различные обобщения классического радикала, а в середине XX века возникла общая теория радикалов колец и алгебр. Радикал – это такой класс идеалов, фактор по которым имеет нулевой радикал и хорошо устроен [1].

Теория радикалов помогает понять структуру алгебраических систем путем разбиения их на полупростые и радикальные, которые уже проще описать. Разработка структурной теории алгебраических систем является актуальной темой современных исследований. В настоящее время опубликованы тысячи работ о построении и исследовании свойств различных радикалов, нашедших многочисленные применения в разных областях современной теории колец и алгебр.

Согласно рабочим программам [2, 3] дисциплин, направленных на изучение актуальных проблем фундаментальной и компьютерной алгебры, наибольшее внимание уделяется таким радикалам колец, как радикал Джекобсона и первичный радикал.

Для ассоциативного кольца R радикал Джекобсона $J(R)$ определяется как множество элементов из R, аннулирующих все неприводимые R-модули, если они существуют, или само кольцо R, если неприводимых R-модулей не существует. Другими словами, $J(R)=\cap A(M)$, где M пробегает все неприводимые R-модули или $J(R)=R$, если неприводимых R-модулей не существует [4, с. 16].

Для построения примеров радикалов колец можно использовать следующую теорему [4, с. 17]: $J(R)=\bigcap\rho$, где ρ пробегает непустое множество N всех максимальных регулярных правых идеалов или $J(R) = R$, если N пусто.

Понятие первичного радикала вводится через первичные идеалы ассоциативного кольца.

Идеал P ассоциативного кольца R называется первичным, если P – собственный идеал и для любых идеалов A и B кольца R из включения $AB\subset P$ следует, что либо $A\subset P$, либо $B\subset P$ [5, с. 94].

Первичный радикал $P(R)$ ассоциативного кольца R определяется как пересечение всех первичных идеалов кольца R [5, с. 96].

Рассмотрим учебные примеры, демонстрирующие поиск радикала Джекобсона и первичного радикала колец. Практика освоения студентами основных понятий теории алгебраических систем показала, что начинать работу с идеалами и радикалами колец удобнее на конечных множествах. Одним из

наиболее исследованных студентами на других дисциплинах конечных колец является кольцо классов вычетов.

Найдем радикал Джекобсона и первичный радикал кольца классов вычетов Z_m, используя теоретические сведения, изложенные в работах [4-5].

Так как в кольце с единицей каждый правый идеал является регулярным, то радикал Джекобсона коммутативного кольца с единицей равен пересечению всех его максимальных идеалов.

Найдем идеалы кольца вычетов. Рассмотрим каноническое разложение числа *m*:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Несобственными идеалами кольца Z_m являются идеалы следующего вида:

$$\overline{p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}} \ , \ 0 \le l_i \le \alpha_i, \ \sum_{i=1}^{k} l_i > 0.$$

Максимальными идеалами кольца Z_m будут идеалы $\overline{p_1}$, $\overline{p_2}$,…, $\overline{p_k}$. Тогда радикал Джекобсона $J(Z_m) = \bigcap_{i=1}^{k} \overline{p_i} = \overline{p_1 p_2 \dots p_k}$.

Например, несобственными идеалами кольца Z_{36} являются множества:

$\overline{0}$,

$\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}, \overline{26}, \overline{28}, \overline{30}, \overline{32}, \overline{34} = \overline{2}$,

$\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}, \overline{30}, \overline{33} = \overline{3}$,

$\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}, \overline{24}, \overline{28}, \overline{32} = \overline{4}$,

$\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30} = \overline{6}$,

$\overline{0}, \overline{9}, \overline{18}, \overline{27} = \overline{9}$

$\overline{0}, \overline{12}, \overline{24} = \overline{12}$,

$\overline{0}, \overline{18} = \overline{18}$.

Тогда идеалы $\overline{2}$ и $\overline{3}$ являются максимальными регулярными и $J(Z_{36}) = \overline{6}$.

Для коммутативного кольца известно, что пересечение всех простых идеалов является первичным радикалом [5, с. 53]. Каждый максимальный идеал коммутативного кольца прост [5, с. 53]. Тогда $P(Z_m) = \bigcap_{i=1}^{k} \overline{p_i} = \overline{p_1 p_2 \dots p_k}$.

В качестве следующего примера найдем радикал Джекобсона и первичный радикал кольца булевых функций от двух переменных.

Будем рассматривать задание булевых функций в виде полинома Жегалкина. Множество булевых функций от двух переменных состоит из следующих элементов: $0,\ 1,\ x_1,\ x_2,\ x_1 \oplus 1,\ x_2 \oplus 1,\ x_1 \oplus x_2,\ x_1 \oplus x_2 \oplus 1,\ x_1x_2,\ x_1x_2 \oplus 1,$ $x_1x_2 \oplus x_1,\ x_1x_2 \oplus x_2,\ x_1x_2 \oplus x_1 \oplus 1,\ x_1x_2 \oplus x_2 \oplus 1,\ x_1x_2 \oplus x_1 \oplus x_2,\ x_1x_2 \oplus x_1 \oplus x_2 \oplus 1.$

Для этого построим несобственные идеалы кольца булевых функций:

$$I_0 = \{0\},$$
$$I_1 = \{0, x_1, x_1x_2, x_1x_2 \oplus x_1\},$$
$$I_2 = \{0, x_2, x_1x_2, x_1x_2 \oplus x_2\},$$
$$I_3 = \{0, x_1 \oplus 1, x_1x_2 \oplus x_2, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\},$$
$$I_4 = \{0, x_2 \oplus 1, x_1x_2 \oplus x_1, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\},$$
$$I_5 = \{0, x_1 \oplus x_2, x_1x_2 \oplus x_1, x_1x_2 \oplus x_2\},$$
$$I_6 = \{0, x_1 \oplus x_2 \oplus 1, x_1x_2, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\},$$
$$I_7 = \{0, x_1x_2\},$$
$$I_8 = \{0, x_1 \oplus 1, x_2 \oplus 1, x_1 \oplus x_2, x_1x_2 \oplus 1, x_1x_2 \oplus x_1, x_1x_2 \oplus x_2, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\},$$
$$I_9 = \{0, x_1x_2 \oplus x_1\},$$
$$I_{10} = \{0, x_1x_2 \oplus x_2\},$$
$$I_{11} = \{0, x_2, x_1x_2, x_1 \oplus 1, x_1 \oplus x_2 \oplus 1, x_1x_2 \oplus x_2, x_1x_2 \oplus x_1 \oplus 1, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\},$$
$$I_{12} = \{0, x_1, x_1x_2, x_2 \oplus 1, x_1 \oplus x_2 \oplus 1, x_1x_2 \oplus x_1, x_1x_2 \oplus x_2 \oplus 1, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\},$$
$$I_{13} = \{0, x_1, x_2, x_1 \oplus x_2, x_1x_2, x_1x_2 \oplus x_1, x_1x_2 \oplus x_2, x_1x_2 \oplus x_1 \oplus x_2\},$$
$$I_{14} = \{0, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\}.$$

Заметим, что $I_0 \subset I_9 \subset I_1 \subset I_{12}$, $I_0 \subset I_{10} \subset I_2 \subset I_{11}$, $I_0 \subset I_{14} \subset I_3 \subset I_8$, $I_0 \subset I_{14} \subset I_4 \subset I_8$, $I_0 \subset I_{14} \subset I_6 \subset I_{11}$, $I_0 \subset I_{14} \subset I_6 \subset I_{12}$. Максимальными идеалами кольца являются I_8, I_{11}, I_{12}. Кольцо является коммутативным с единицей. Тогда радикал Джекобсона $J(R) = I_8 \bigcap I_{11} \bigcap I_{12} = I_0 = \{0\}$. Аналогично находится и первичный идеал кольца булевых функций, то есть $P(R) = I_8 \bigcap I_{11} \bigcap I_{12} = I_0 = \{0\}$.

В качестве примера поиска радикалов некоммутативного кольца рассмотрим кольцо матриц второго порядка над полем F_2.

Правыми идеалами кольца являются следующие идеалы:

$$I_0 = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\},\ I_1 = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\right\},$$
$$I_2 = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\right\},\ I_3 = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right\}.$$

Тогда радикал Джекобсона $J(R) = I_1 \bigcap I_2 \bigcap I_3 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$.

Для построения первичного радикала нам понадобится таблица умножения идеалов I_1, I_2 и I_3 кольца (таблица 1).

Таблица 1 – Таблица умножения идеалов

$I_k I_s$	I_1	I_2	I_3
I_1	I_1	I_1	I_1
I_2	I_2	I_2	I_2
I_3	I_3	I_3	I_3

Согласно определению первичными идеалами кольца являются I_1, I_2 и I_3. Тогда первичный радикал $P(R) = I_1 \bigcap I_2 \bigcap I_3 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$.

В заключение отметим, что построение радикалов конечных колец помогает обучающимся лучше понять структуру радикала и его предназначение. Приведенные примеры позволяют проиллюстрировать такие понятия как идеал, максимальный идеал, первичный идеал, радикал Джекобсона, первичный радикал. Кроме того, дискретность и конечность приведенных в статье колец позволяет автоматизировать процесс построения основных алгебраических структур с помощью разработки компьютерных программ.

Список литературы

1. Пихтильков, С.А. Структурная теория специальных алгебр Ли / С.А. Пихтильков. – Оренбург, ОГУ. – 2013. – 171 с.

2. Рабочая программа дисциплины «Б.1.В.ДВ.4.1 Актуальные проблемы фундаментальной и компьютерной алгебры» / сост. О.А. Пихтилькова, А.Н. Благовисная. – Оренбург: ОГУ, 2018.

3. Рабочая программа дисциплины «А.1.В.ОД.2 Математическая логика, алгебра и теория чисел» /сост. С.А. Пихтильков, Е.В. Мещерина – Оренбург: ОГУ, 2017.

4. Херстейн, И. Некоммутативные кольца / И. Херстейн. – М.: Мир, 1972. –192 с.

5. Ламбек, И. Кольца и модули / И. Ламбек. – М.: Изд-во «Факториал Пресс», 2005. – 283 с.

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛЕЙ РАЗНОЧАСТОТНЫХ ВРЕМЕННЫХ РЯДОВ НА ПРИМЕРЕ УРОЖАЙНОСТИ ЗЕРНОВЫХ КУЛЬТУР

Болодурина И.П., д-р. техн. наук, профессор,
Парфёнов Д.И., канд. техн. наук,
Пивоварова К.В.
Оренбургский государственный университет

На сегодняшний день большинство развивающихся стран достаточно сильно зависят от продуктивности сельского хозяйства и как следствие данного процесса от урожайности пахотных земель. В свою очередь негативные влияния глобального потепления оказывают существенное воздействие на результативность возделывания зерновых культур. Это напрямую сказывается на благосостоянии населения и экономическом развитии стран. Регионы с резко континентальным климатом особенно уязвимы к потенциальному ущербу от агроклиматических и экологических изменений. Это связано с высокой динамикой изменения погодных условий за короткий период времени в этих регионах.

Поэтому в качестве объекта настоящего исследования нами выбрана сухостепная зона России, Оренбургская область, являющиеся одним из лидеров рынка по производству зерновых культур. Резкоконтинентальный климат региона обусловлен расположением Оренбургской области в глубине материка и особенностями рельефа. Отличительной чертой рассматриваемого региона является холодная продолжительная зима и жаркое сухое лето. Осадки вегетационного периода сельскохозяйственных культур неустойчивы, в то время как переходы от зимы к лету очень короткие.

На протяжении нескольких последних лет исследованию влияния климата на урожайность сельскохозяйственных культур уделяется особое внимание. В большинстве исследований оценивается степень, в которой варианты адаптации могут уменьшить ожидаемое воздействие изменения климата. В качестве факторов, влияющих на урожайность, рассматривается такие блоки факторов как природно-климатические, экономические и социальные. Под природно-климатическими факторами обычно подразумевают плодородие и механический состав почвы, температурный режим, уровень грунтовых вод, количество осадков, обогащенность местности кислородом и другие. К экономическим факторам относят количество, качество и структура вносимых удобрений; качество и сроки выполнения всех полевых работ; качество посевного материала; изменение сортового состава посевов; известкование и гипсование почвы; борьба с болезнями и вредителями растений; чередование культур в полях севооборота и др.

Анализ научных работ, связанных с исследованием урожайности зерновых культур позволил сформировать информационную базу, а также осуществить комплексный подход к выбору методологии исследования. При построении

математических моделей урожайности сельскохозяйственных культур, выращиваемых в открытом грунте, может быть предъявлен ряд требований. Производителя сельскохозяйственных культур урожайность интересует с точки зрения учета параметра времени. Соответственно при построении математических моделей следует применять анализ временных рядов.

Существуют различные подходы к анализу временных рядов. Однако, большинство из них имеют определенные ограничения. В рамках данной работы, мы предлагаем гибридный алгоритм построения модели, который, используя хорошо изученный популярных методов оценки временных рядов, позволяет создать устойчивую прогнозную систему.

Сингулярный спектральный анализ успешно применяемый метод в различных областях наук от метеорологии и астрономии до био-информатики. Этот метод позволяет сжать информацию, сгладить временные ряды, а также спрогнозировать их дальнейшую динамику. После получения информации о характере временных рядов, следует учитывать его при спецификации моделей.

Панельные данные представляют собой временные ряды одного набора экономических факторов, измеренные для различных объектов. Панельные данные насчитывают три измерения: признаки (переменные) – объекты – время. Преимущества анализа панельных данных перед другими методами заключается в том, что благодаря специальной структуре панельные данные позволяют строить более гибкие и содержательные модели и получать ответы на вопросы, которые недоступны только в рамках, например, моделей, основанных на пространственных данных. Возможность построения моделей с фиксированными и случайными индивидуальными эффектами позволяют оценивать отличия между экономическими единицами, что нельзя сделать в рамках стандартных регрессионных моделей.

Однако интерес представляет построение регрессионных моделей, которые объединяют данные с различными частотами дискретизации. На общем уровне интерес к регрессиям MIDAS часто затрагивает ситуацию на практике, когда соответствующая информация является высокочастотными данными, тогда как переменная, представляющая интерес, отбирается на более низкой частоте. Например, при моделировании урожайности, низкочастотная переменная это урожайность, измеренная ежегодно, в то время как климатические и погодные данные представляют собой низкочастотную информацию, так как большинство погодных данных измеряется ежедневно, а также декадно и ежемесячно.

В рамках проведенного исследования на первом шаге осуществляется сингулярный спектральный анализ временных рядов, определяется структура ряда. На втором этапе реализовано оценивание двух типов моделей MIDAS и модели на панельных данных. С помощью ретроспективного моделирования принимается решение о том, какой тип модели лучше подходит под текущий набор исходных данных. Затем, на третьем этапе происходит уточнение модели, выбранной на предыдущем шаге. Если выбрана модель MIDAS, то посредством имитационного моделирования происходит подбор частотных регрессоров. Если же выбрана модель на панельных данных, то происходит сравнение моделей с

фиксированными и случайными случайными эффектами. На выходе имеем обоснованную спецификацию модели, имеющую наибольшую точность по сравнению с исследованием моделей целого класса.

Для исследования временных рядов и прогноза урожайности в рамках настоящего исследования выбраны 4 посевные зоны Оренбургской области: d_{1_i} – Бузулукский район; d_{2_i} – Соль-Илецкий район; d_{3_i} – Чебеньки; d_{4_i} – Тоцкое. В рамках данной статьи произведена иллюстрация работы алгоритма на примере урожайности в Бузулукском районе. С помощью стандартных статистических тестов доказана нестационарность временного ряда, а также наличие тренда и сезонных компонент. Для того чтобы отделить накладывающиеся друг на друга сезонные колебания, а также определить периоды смены поведения линии тренда проведен сингулярный спектральный анализ временного ряда. В исследуемом временном ряде присутствует нелинейный тренд с переменчивой структурой (рисунок 1 и 2), что говорит о том, что на данный ряд не является рядом авторегрессии, а зависит и от изменения сторонних факторов.

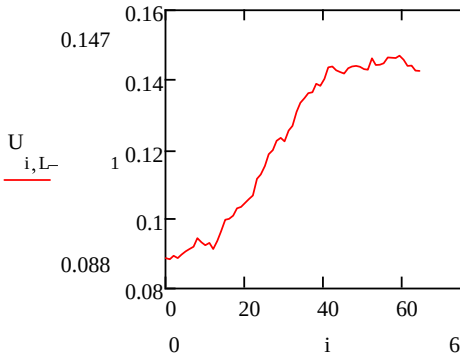
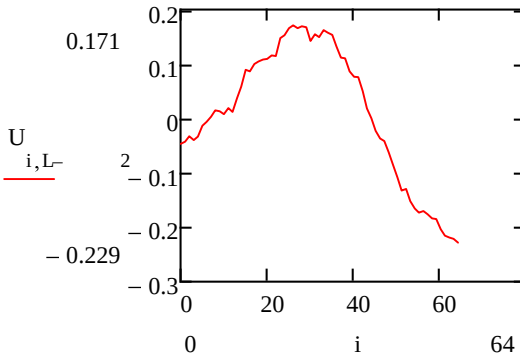


Рисунок 1 – первая сингулярная тройка



РРисунок 2 – вторая сингулярная тройка

Также можем заметить, что присутствуют регулярные колебания на графиках последующих сингулярных троек, что говорит о наличии сезонности с различной частотой, но для подтверждения этого предположения необходимо построить двумерные изображения. Примеры идентификация гармоник с помощью двумерных диаграмм представлена на рисунках 3 и 4.

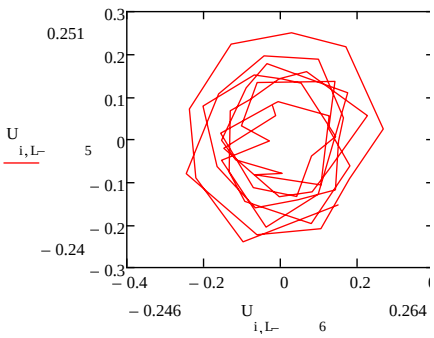


Рисунок 3 – Двумерная диаграмма 3 и 4 гармоник

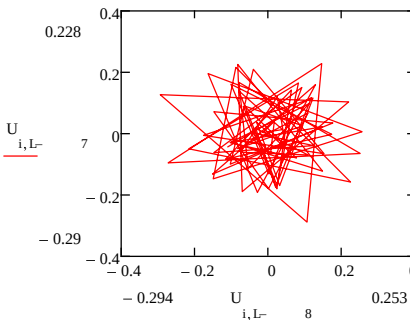


Рисунок 4 – Двумерная диаграмма 6 и 7 гармоник

На рисунках 3 и 4 различимы регулярные двумерные изображения, образующие траектории с вершинами, лежащими на кривой спиралеобразной формы. Таким образом, можем сделать вывод о том, что в рассматриваемом ряду присутствует несколько гармоник. Причем они отделимы и имеют различный период колебаний. Для того, чтобы определить период колебаний, был построен график логарифмов собственных чисел траекторной матрицы, представленный на рисунке 5.

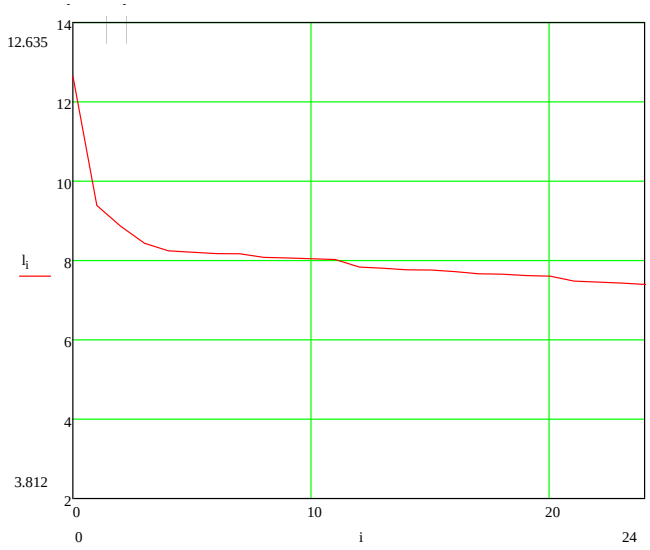


Рисунок 5 – График логарифмов собственных чисел траекторной матрицы,

На рисунке 5 отчетливо заметны «ступеньки», что говорит о наличии отделимых гармоник. Причем периоды сезонности составляют 3 года, 6 и 12 лет. А также несколько более мелких, шумовых гармоник, которые можно отнести к волатильности урожайности. Использование сингулярного спектрального анализа позволяет увидеть наслоение гармоник с кратными периодами колебаний.

При проведении аналогичного спектрального разложения для временного ряда осадков в оренбургской области в рассматриваемом периоде были получены принципиально иные результаты. Например, в данном случае сделать вывод о наличии тренда не представляется возможным, так как первые сингулярные тройки имеют рваный вид и не соответствуют ни гармоникам, ни монотонно ведущим себя числовым рядам. Заметить регулярные колебания на нескольких графиках, но они требует более детальной проверки: построение двумерных изображений. Однако на построенных графиках нельзя различить регулярные двумерные изображения, образующие двумерные траектории с вершинами, лежащими на кривой спиралеобразной формы. Таким образом, можем сделать предположение о том, что гармоник в ряду нет (сезонности не наблюдается). Данное предположение идет вразрез с большим количеством исследований данной тематики, поэтому проведено дополнительное исследование, так как логично предположить, то при выбранных параметрах происходит смешивание компонент ряда, порожденное отсутствием сильной

разделимости. Детальный анализ графиков логарифмов собственных чисел новой тракторной матрицы позволил сделать вывод о наличии отделимой сезонной компоненты. Медленное, почти без скачков убывание собственных значений говорит о наличии шума в сигнале. Также подтверждением правильности разделения сигнала и шума является проверка на принадлежность к шуму компоненты ряда, полученной по «шумовым» собственным тройкам, стандартными статистическими методами.

Таким образом, при анализе исходного временного ряда пришлось столкнуться с проблемой перемешивания компонент ряда, то есть с проблемой отсутствия сильной разделимости, вызванной близкими собственными числами, соответствующим разным компонентам. Однако, стоит заметить, что рассматриваемый временной ряд является достаточно специфичным в связи с сильной волатильностью рассматриваемых значений, ведь нередко после затяжной засухи выпадает рекордное количество осадков, что вызывает осложнения при анализе числовой информации только осадков, без учета температуры воздуха и атмосферного давления. Однако, в результате исследовании обоих временных рядов (осадков и урожайности) удалось выявить сезонность периодами кратными трём.

С учетом выявленные структурных особенностей проведена апробация MIDAS модели на основе данных об урожайности яровой пшеницы в Бузулукском районе Оренбургской области, а в качестве регрессоров такие декадные данные метеоусловий как средняя температура воздуха, влажность воздуха, процент осадков от нормы, промерзание почвы и высота снега. Оценивание коэффициентов модели произведено с помощью языка программирования Python и дополнительного пакета midaspy с помощью нелинейного метода наименьших квадратов. Результатом оценивания служит сильно разряженная матрица коэффициентов, при этом к оцениваемым параметрам также относятся и величины лагов при объясняемой переменной.

Анализ блока коэффициентов, отвечающих за лаговые значения зависимой переменной, показал, что урожайность текущего периода зависит от урожайности предыдущего года прямо пропорционально с положительным знаком. Что свидетельствует, о том, что урожайность текущего периода зависит от качества посевных культур, являющимися результатом урожайности предыдущего периода.

Анализ блока коэффициентов отвечающих за количество осадков подтвердил гипотезу о влиянии. Значимыми лаговыми переменными оказались переменные осенних и весенних периодов. Также, лаговые переменные температуры воздуха значимыми оказались для весенних и осенних периодов, о чем свидетельствует анализ блока коэффициентов. Показатель влажность воздуха значим только в летнем периоде. А в зимние периоды оказался положительно значим показатель высоты снега.

Поскольку данные измерены как в пространстве, так и во времени, то практический интерес представляют модели панельных данных.

В качестве зависимой переменной выступает урожайность зерновых культур, объектами выступают районы Оренбургской области (Бузулукском, Соль-Илецком районах, Чебеньки, Тоцкое), к регрессорам относятся влажность воздуха (%), скорость ветра (м/с), атмосферное давление (гПа), объемное содержание кислорода в воздухе (г/м3), снежный покров, осадки, температура воздуха (°C), а также их квадраты. Так как в результате спектрального анализа и построенной модели MIDAS выявлено наличие сезонных компонент, то к факторам осадки и температура воздуха добавим мультипликативно коэффициент сезонности, чтобы определить степень влияния. Общий вид регрессионной модели с фиксированными записывается как:

В результате модели получили двунаправленную модель с фиксированными эффектами, то есть значимы не только индивидуальные природно-климатические особенности муниципальных образований, но и временные эффекты.

Таким образом, результаты показывают, что большинство квадратов климатических переменных значимы ежегодно и сезонно на уровне 1% значимости, что подразумевало, что климат оказывает нелинейное влияние на продуктивность зерновых культур.

В результате произведенного исследования разработана методология интерактивного мониторинга агроклиматических факторов, оказывающих влияние на урожайность зерновых культур в сухостепной зоне России на примере Оренбургской области с учетом географических и отраслевых особенностей. Применение эконометрических модели, построенной на разночастотных данных, позволило определить структурные влияния на урожайность в течение всего года, а также учитывая ключевые вегетативные периоды зерновых культур. Кроме того, в результате исследования с помощью языка программирования Python разработано универсальное программное средство, позволяющее быстро производить оценку моделей, не только в рамках предметной области урожайности, но и на примере других данных, в которых важным фактором является динамическая взаимосвязь различных показателей во времени. Таким образом, установлено что, предложенный подход, основанный на проведении агрегации результатов сингулярного спектрального анализа, позволяет сэкономить время для подбора спецификации модели.

Разработанное программное средство, реализующее предложенную нами методологию исследования, позволяет автономно и динамически оценивать уточненные на актуальных данных модели. При этом, для исследователя упрощается задача интерпретации полученных результатов, так как перед ним предстает полная картина взаимосвязей, присутствующая в исходных данных: сингулярный спектральный анализ позволяет увидеть сезонность и зависимость исследуемых факторов от времени, в то время как оцениваемая модель позволяет судить о взаимосвязи между факторами, открывая доступ к информации, способной помочь влиять на исследуемый фактор, а также делать более точные прогнозы.

Список литературы

1. Максютов Н.А., Жданов, В.М., Лактионов О.В. Биологическое и ресурсосберегающее земледелие в степной зоне Южного Урала. 2-е доп. изд. Оренбург: ООО «Печатный дом «Димур», 2008. 232 с.

2. Ковтун В.И. Влияние селекции на качество зерна на юге России // Известия Оренбургского государственного аграрного университета. 2010. № 27-1. С. 9-11.

3. Бюллетени о состоянии сельского хозяйства [Электронный ресурс] // Каталог публикаций: Федеральная служба государственной статистики. 2018. 10 ноября. url:http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/publications/catalog/doc_1265196018516 (дата обращения: 10.11.2018).

4. Eyshi E.R. Effects of heat and drought stress on cereal crops across spatial scales: дис. канд. фил. наук. Бонн, 2016.

5. Ontel I., Vladut A. Impact of drought on the productivity of agricultural crops within the Oltenia Plain, Romania // Geogr. Pannonica. 2015. 19(1). P. 9-19.

6. Cereal productivity in west africa: a panel data analysis / M.I. Adah, O. K. Omolade, C.V. Iwuoha // American Journal of Business, Economics and Management. 2017. 5(4). P. 38-43.

7. Metaksa O.B. Impact of weather variations on cereal productivity and influence of agroecological differences in ethiopian crop production // East Africa Research Papers in Economics and Finance. 2016. 7. P. 1-36.

8. The Impact of Global Warming on Agriculture: A Ricardian Analysis Robert Mendelsohn, William D. Nordhaus and Daigee Shaw // The American Economic Review. 1994. 84(4). P. 753-771.

9. George T. Why crop yields in developing countries have not kept pace with advances in agronomy // Global Food Security. 2014. 3(1). P. 49-58. doi: 10.1016/j.gfs.2013.10.002

10. Temperature increase reduces global yields of major crops in four independent estimates / Z. Chuang, L. Bing, P. Shilong, W. Xuhui, D.B. Lobell, H. Yao etc. // Proceedings of the National Academy of Sciences. 2017. 114(35). P. 9326-9331. doi: 10.1073/pnas.1701762114

11. Аксарина Е.А., Пасов В.М. Прогноз урожайности яровой пшеницы до сева в Казахстане на основе использования особенностей развития циркуляции в атмосфере // «Экспресс-информация» ВНИИГМИ-МЦД. 1978. Вып. 1(51). С. 12-20.

12. Ермакова Л.Н., Толмачева Н.И. Прогноз урожайности яровой пшеницы на Урале синоптико-статистическим методом // Географический вестник. 2006. 2(4). С. 111-114.

13. Bollen K.A., Brand J.E. A general panel model with random and fixed effects: a structural equations approach // Social Forces. 2010. 89(1). P. 1-34.

НАДЕЖНОСТЬ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Бурькова Е. В., канд. пед. наук, доцент
Оренбургский государственный университет

В современных условиях конкуренции и постоянно меняющихся угроз безопасности обеспечение надежности функционирования системы физической защиты объектов информатизации является актуальной задачей. Оценка надежности системы физической защиты входит в процесс аудита уровня защищенности контролируемого объекта. В связи с этим важной и актуальной является задача построения алгоритмов вычисления показателей надежности системы физической защиты.

Системы физической защиты представляют собой совокупность физических, инженерно-технических, организационных мероприятий и действий подразделений охраны, предназначенных для защиты объекта от несанкционированных действий нарушителя (предотвращения диверсий или хищений носителей конфиденциальной информации и материальных средств). Основными функциями физической защиты является обнаружение проникновения, задержка и нейтрализация нарушителя. В соответствии с этим в состав системы физической защиты входят следующие функциональные подсистемы:

- охранной сигнализации;
- контроля и управления доступом;
- теленаблюдения;
- оперативной связи и оповещения;
- электропитания, освещения.

Под надежностью физической защиты понимают обеспечение требуемого уровня безопасности объекта независимо от внешних и внутренних воздействий. Надежность защиты обеспечивается при условии безотказной работы средств системы защиты. Методы и средства физической защиты должны надежно перекрывать возможные пути несанкционированного доступа к охраняемым ресурсам, независимо от формы их представления, языка выражения и вида физического носителя. Неисправности и сбои в работе технических средств защиты могут привести к высоким ущербам для защищаемого объекта. Ложные срабатывания средств защиты при отсутствии угрозы менее опасны, однако они способствуют ослаблению бдительности персонала охраны [1].

В соответствии с теорией надежности технических систем основными показателями являются вероятность безотказной работы, время наработки на отказ, интенсивность отказов, коэффициент готовности, коэффициент восстанавливаемости и другие. В применении к системе физической защиты при выборе показателей надежности необходимо выполнить следующие требования:

- показатель должен иметь определенный физический смысл;
- должна быть обеспечена возможность его количественной оценки;

− показатель должен иметь форму для вычисления результирующей оценки надежности системы;

− должен быть разработан алгоритм оценки данного показателя;

− показатель должен отражать какую-либо из значимых сторон функционирования системы физической защиты (СФЗ) [4].

Исследования надежности систем физической защиты проводились многими учеными. Дурденко В.А., Рогожин А.А. провели математическое моделирование охранной телевизионной системы, в качестве показателя надежности ими использованы время наработки на отказ каждого прибора (из технической документации), время восстановления работоспособного состояния оборудования (определяется методом испытаний), комплексный показатель – коэффициент готовности к выполнению целевой функции. В основе расчета проводилось разработка схемы функциональной целостности системы охранного телевидения и построение логической математической модели работоспособности этой системы [2]. В работе Пономарева А.А. в качестве показателей надежности системы защиты рассматриваются отказы (сбои) технических и программных средств обеспечивающих защиту информации и вероятность нахождения злоумышленником уязвимостей в системе защиты информации. Для исследования строится графовая модель, в качестве результата анализа надежности определяется время преодоления нарушителем средств защиты [5]. В работе Мельникова А.В. рассчитан вероятностный критерий оценки надежности элемента системы физической защиты, основанный на учете уровня возможной угрозы проникновения и способности системы защиты выполнять свои функции. Вероятность безотказной работы элемента защиты за время t есть функция надежности. Для решения поставленных задач в работе использовались теория вероятностей и математическая статистика, теория надежности, теория графов, комбинаторный анализ, методы математического моделирования.

При разработке математической модели оценки надежности системы физической защиты объекта информатизации используется логико-вероятностный метод, основные этапы метода:

− ввод исходных данных;

− построение схемы функциональной целостности;

− формулирование критериев функционирования, параметров элементов подсистем;

− построение структурной схемы системы физической защиты с учетом разделения на подсистемы и связи между ними;

− определение перечня показателей надежности;

− построение формализованной модели расчета показателей надежности;

− проведение вычислительного эксперимента по расчету оцениваемых показателей надежности.

Определяется перечень функций системы физической защиты, к которым предъявляются требования с точки зрения надежности, определяется состав

технических средств, участвующих в реализации функций СФЗ. Строится структурно-логическая схема расчета надежности, которая состоит из последовательно-параллельно соединенных технических средств, участвующих в реализации функций СФЗ.

Безотказность – это свойство системы сохранять работоспособность в течение требуемого интервала времени непрерывно без вынужденных перерывов.

При расчете показателей принимаются допущения:

– вероятность безотказной работы СФЗ в течение времени t не зависит от момента начала работы;

– функция распределения времени наработки на отказ и времени восстановления подчиняется экспоненциальному закону;

– контроль состояния технических средств СФЗ непрерывный;

– обслуживание осуществляется при неограниченном восстановлении.

Анализ показателей надежности целесообразно проводить для отдельных подсистем с учетом способа их соединения в схеме. Наиболее часто используемые показатели надежности систем физической защиты приведены в таблице.

Таблица – Характеристика показателей надежности СФЗ

Показатель	Формализованное описание	Краткая характеристика
Наработка на отказ (в единицах времени)	В расчетах Т берется из норм технических условий на устройства $T = \int_0^\infty t a(t)\,dt = \int_0^\infty P(t)\,dt$	Время непрерывной работы устройства до первого отказа, определяется как математическое ожидание времени работы устройства до отказа
Интенсивность отказа элемента СЗИ в нормальных условиях эксплуатации	$\lambda = \frac{1}{T}$	Вероятность отказа устройства в единицу времени после данного момента t, при условии, что до него отказ не возникал
Коэффициент готовности (Кг) к выполнению целевой функции	$K_{ГЭ} = \frac{T}{T + T_{В}}$ Тв –время восстановления	вероятность того, что аппаратура будет работоспособна в произвольный момент времени t и безотказно проработает заданное время

Интенсивность восстановления	$\mu = \frac{1}{T_B}$ Тв –время восстановления	Восстанавливаемость: свойство системы, заключающееся в ее приспособленности к предупреждению, обнаружению и устранению причин возникновения отказов, а также поддержанию и восстановлению работоспособного состояния путем проведения технического обслуживания и ремонтов
Вероятность безотказной работы	$P_{(t)} = e^{\frac{-t}{T}}$	Вероятность безотказной работы в течение заданного времени t

Вероятность работоспособного состояния системы, состоящей из n элементов определяется по формуле:

$$P_c = P_1 P_2 \ldots P_n = \prod_{i=1}^{n} P_i$$

Поэтому чем сложнее система, чем больше в ней элементов, соединенных последовательно, тем ниже будет вероятность безотказной работы.

Комплексный показатель надежности СФЗ будет определяться рядом факторов: конструктивных, производственно-технологических, эксплуатационных и других. Многообразие факторов, определяющих надежность имеют вероятностно-временной характер, так как происходят неконтролируемые изменения свойств системы, приводящие к модификации характеристик элементов и отказам составляющих СФЗ. В соответствии с этим надежность систем физической защиты описывается вероятностно-статистическими характеристиками. Надежность является внутренним свойством системы защиты, которое расчитывается при ее проектировании и проявляющимся во времени при эксплуатации. В связи с этим в процессе функционирования система защиты может находиться в одном из состояний, при этом каждое из них характеризуется определенным уровнем надежности, т.е. переход из одного состояния в другое определяется показателями надежности системы защиты [6]. Для исследования надежности системы физической защиты наиболее целесообразным представляется использования графового метода. Необходимо построить ориентированный граф, вершинами которого являются состояния СФЗ (работоспособное и неработоспособное), а направленные ребра – интенсивности и направления возможных переходов - интенсивность потока отказов, интенсивность потока восстановлений работоспособности СФЗ.

Проведение расчетов по определению вероятностей состояния СФЗ проводят с помощью различных программных пакетов, например пакет MathCAD.

Результатом проведения оценки надежности СФЗ является выявление наиболее подверженных отказам и сбоям элементов системы защиты. Для повышения уровня надежности используют резервирование таких элементов, либо включают в систему защиты дополнительные технические средства, что обеспечивает снижение риска реализации угроз безопасности для защищаемого объекта.

Список литературы

1. Бурькова, Е.В. Физическая защита объектов информатизации: учебное пособие / Е.В. Бурькова, – Оренбургский гос. ун-т. – Оренбург: ОГУ, 2017. – 157 с.

2. Дурденко В. А., Рогожин А. А. Математическое моделирование и оценка надежности охранной телевизионной системы отдела полиции. Вестник ВГУ– № 4. –2015. – С. 44-54.

3. Лужаева Е. М. Модель количественной оценки надежности технической системы / Е. М. Лужаева, Е. Н. Яговкина, Т. Ю. Фрезе // Вектор науки Тольяттинского государственного университета – № 2. – 2016. - С. 35-39.

4. Мельников А.В. Модели оценки надежности системы охраны объектов в условиях целенаправленного противодействия охранным функциям: автореферат дис. ... кандидата технических наук : 05.13.18 / Воронеж. ин-т МВД России. - Воронеж, 2004. - 16 с.

5. Пономарёв А. А. Оценка надежности систем защиты информации/ А.А. Пономарев //Телекоммуникационные устройства и системы. – № 4. – 2014. – С. 431-432.

6. Шлаев Д.В. Исследование функциональных состояний информационной системы с целью улучшения ее надежности / Д.В. Шлаев, Д.Н. Резеньков, Д.В. Гайчук // Фундаментальные исследования. – № 10. – 2016 С. 364-367.

ПЕЧАТНЫЕ ПЛАТЫ В КУРСОВОМ ПРОЕКТИРОВАНИИ ПО ИНЖЕНЕРНОЙ И КОМПЬЮТЕРНОЙ ГРАФИКЕ

Ваншина Е.А., канд. пед. наук, доцент,
Ваншин В.В., канд. с.-х. наук, доцент
Оренбургский государственный университет

Применение печатных плат с использованием современных систем автоматизированного проектирования (САПР) в производстве изделий приборостроения, средств вычислительной техники, радиоэлектронной аппаратуры обеспечивает автоматизацию монтажно-сборочных операций, снижает габаритные размеры аппаратуры, металлоемкость и повышает конструктивные и эксплуатационные качества изделия.

Цель работы – создание комплекта заданий «Платы печатные» для методических указаний к курсовому проекту по инженерной и компьютерной графике для изучения обучающимися требований стандартов к выполнению чертежей печатных плат, ее элементов, приобретение теоретических знаний в области проектирования печатных плат, формирования общепрофессиональных и профессиональных компетенций бакалавров направления подготовки 11.03.03 Конструирование и технология электронных средств профиля «Проектирование и технология радиоэлектронных средств».

Сформированный комплект заданий по печатным платам в системе КОМПАС необходим для получения последующей конструкторско-технологической документации: сборочного чертежа печатных узлов, спецификаций к ним.

Удобным решением для автоматизации черчения является система КОМПАС-3D как инструмент для создания трехмерных ассоциативных моделей отдельных деталей, сборочных единиц и чертежей, содержащих оригинальные и стандартизованные конструктивные элементы.

Один из компонентов САПР КОМПАС – это чертежно-графический редактор для автоматизации проектно-конструкторских работ. Базовый функционал системы включает в себя также возможность получения конструкторской и технологической документации. Простой понятный интерфейс, обширная справочная система и наличие интерактивного обучающего руководства «Азбука КОМПАС» способствуют легкому и быстрому освоению работы в системе.

К этапам проектирования электронных средств относятся: 1) ввод принципиальной схемы; 2) моделирование схемы; 3) упаковка схемы на печатную плату; 4) размещение компонентов на печатной плате; 5) получение конструкторской документации; 6) получение информации для производства плат на технологическом оборудовании.

Известно, что печатная плата (ПП), плоское изоляционное основание с отверстиями с нанесенными на одной или на обеих сторонах проводниками согласно электрической схеме изделия, служит для монтажа на них

электрорадиоэлементов (ЭРЭ) при помощи полуавтоматической или автоматической установки и последующей пайки.

Комплекты для приборостроения и есть такие инструменты КОМПАС-3D. Это необходимые и полнофункциональные наборы специализированных пакетов и приложений, которые объединены общей идеей автоматизации проектирования радиоэлектронной аппаратуры и электрооборудования.

Чертеж печатной платы, созданный в КОМПАС, предполагает существование исходного готового проекта печатной платы. Схема электрическая принципиальная проектируется в модуле схем с внедрением электронных компонентов из единых библиотек, затем посредством трансляции данных (списка соединений) в модуле печатной платы автоматически размещаются электронные компоненты в соответствии со схемой электрической принципиальной. Также в проекте печатной платы можно применять единые библиотеки. Электронные компоненты размещаются (вручную или автоматизировано) в рамках контура печатной платы. Далее осуществляется ручная, полуавтоматическая или автоматическая трассировка проводников с помощью программы – автотрассировщика. Модули символов, корпусов и библиотек служат соответственно для создания символов, посадочных мест и наполнения компонентов в единые библиотеки электронных компонентов.

Результат проектирования радиоэлектронных устройств (РЭУ) – готовая схема РЭУ и данные проектирования печатной платы. Необходим также комплект конструкторской документации, состоящий из схемы электрической принципиальной (Э3), перечня элементов (ПЭ3), чертежа печатной платы (ПП), сборочного чертежа РЭУ и спецификации к нему.

В системе КОМПАС-3D нами построены 17 вариантов и образец задания «Печатные платы» для методических указаний к курсовому проекту по инженерной и компьютерной графике для студентов, обучающихся по программам высшего образования по направлению подготовки 11.03.03. Пример одного из вариантов и образец выполнения задания приведены на рисунках 1 и 2.

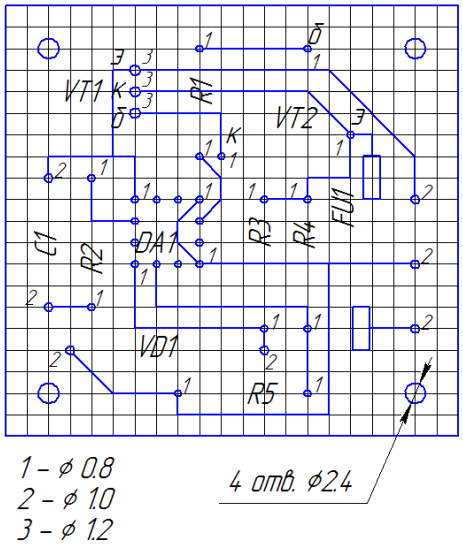


Рисунок 1. Пример одного из вариантов графической части

курсового проекта «Платы печатные»

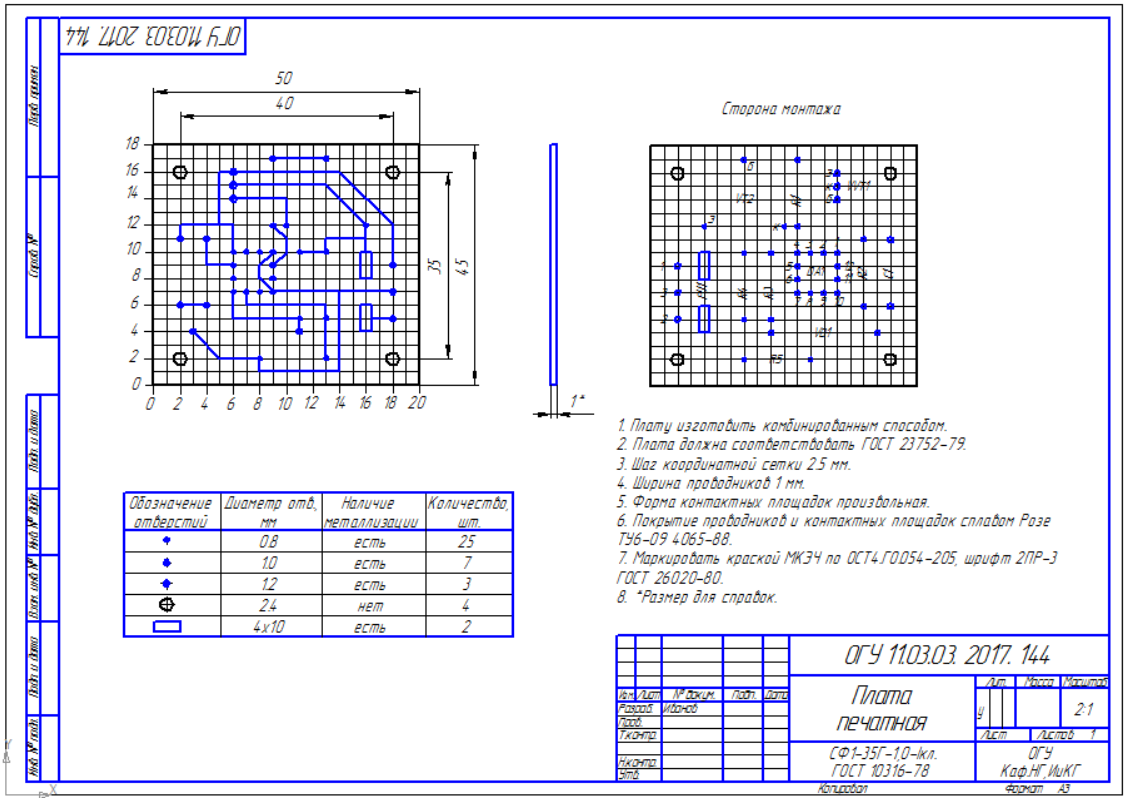


Рисунок 2. Образец выполнения графической части курсового проекта «Платы печатные»

Для формирования комплекта заданий использовалось плоское компьютерное геометрическое моделирование в 2D-подсистеме САПР, в которой векторные геометрические модели созданы на основе построения по заданным отношениям и с использованием преобразований. При построении с использованием отношений последовательно задавался создаваемый примитив, список отношений и примитивы, к которым даны отношения. В процессе построения с использованием преобразований приводился вначале преобразуемый объект, затем – преобразование, далее – выполнение преобразования с помощью аналитических расчетов и операций с векторной математической моделью.

Практическая значимость работы заключается в построении в системе КОМПАС-3D на основе плоского моделирования наглядного комплекта заданий «Платы печатные» из 17 вариантов для методических указаний по выполнению курсового проекта [2] по инженерной и компьютерной графике, что способствует оптимизации учебного процесса по геометро-графическим дисциплинам, сформировать общепрофессиональные и профессиональные компетенции бакалавров направления подготовки 11.03.03 Конструирование и технология электронных средств профиля «Проектирование и технология радиоэлектронных средств», необходимые для освоения последующих специальных дисциплин, при выполнении курсовых работ и дипломного

проекта.

Список литературы

1. Александров К. К., Кузьмина Е. Г. Электротехнические чертежи и схемы / К. К. Александров, Е. Г. Кузьмина. – М.: Энергоатомиздат, 1990. – 282 с.

2. Ваншина, Е. А. Платы печатные: методические указания к курсовому проекту / Е. А. Ваншина. – Оренбург: ОГУ, 2017. – 45 с.

3. Ваншина, Е. А. Проблемы компьютеризации преподавания графических дисциплин / Е. А. Ваншина // Вестник Оренбургского государственного университета. – 2009. – №2. – С.143. – ISSN 1814-6457.

4. Конструирование и технология печатных плат: учебное пособие для радиотехнических специальностей вузов / А. Т. Жигалов, Е. П. Котов, К. Н. Шихаев, Б. А. Хохлов. – М.: Высш.шк., 1973. – 216 с.

5. Лашкова Н. А. Начертательная геометрия и инженерная графика: чертежи и схемы по специальности: учебно-методическое пособие для учащихся / Н. А. Лашкова. – 3-е изд., испр. – Минск: МГВРК, 2011. – 86 с.

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ОТ BOT NET

Викулов Д.В., Влацкая И.В., канд. техн. наук, доцент
Оренбургский государственный университет

Современные технологии динамично развиваются, пользователям сети Интернет уже давно доступно создание персональных страниц. Но так же быстро развиваются знания и навыки людей, которые преследуют злой умысел. Любая персональная страница пользователя в Интернете может стать жертвой Bot Net – компьютерной сети, состоящей из огромного множества зараженных устройств с доступом в Интернет. Каждое устройство способно по команде злоумышленника рассылать спам, перебирать пароли, а также осуществлять многократные попытки доступа к персональной странице пользователя. Злоумышленник удаленно управляет зараженными машинами каждой по отдельностью, частью устройств, входящих в сеть, или всей сетью целиком.

Распространение технологий широкополосного доступа к сети Интернет привело к колоссальному расширению возможностей Bot Net по запуску атак типа «отказ в обслуживании», заражению миллионов устройств вредоносным кодом, хищению конфиденциальных данных, «накручиванию» клик-счетчиков, широкомасштабной рассылке спама, перебору паролей на удаленной системе, поисковому спаму и фишингу. Причем Bot Net позволяет осуществлять вплоть до всех перечисленных видов деятельности одновременно.

Боты, как таковые, не являются вирусами. Они представляют собой набор программного обеспечения, который может состоять из вирусов, брандмауэров, программ для удаленного управления компьютером, а также инструментов для скрытия от операционной системы.

На сегодняшний день Bot Net является основной угрозой безопасности в сети Интернет. Атаку легко заказать, злоумышленники очень быстро находят новые уязвимости устройств и сайтов. А самое важное, что Bot Net сложно обнаружить, так как их топология динамичная, что позволяет обходить наиболее распространенные средства защиты.

Существует множество публикаций как отечественных, так и зарубежных авторов, посвященных изучению Bot Net и методов борьбы с такой сетью. В монографиях, статьях и книгах, в которых рассматриваются Bot Net, отражаются следующие направления исследований:

- анализ деятельности Bot Net [2, 8, 14, 16];
- причины создания Bot Net [1, 10, 11-13], в число которых входит проведение DDoS-атак, рассылка спама, сбор конфиденциальной информации, а также создание поискового спама;
- методы создания Bot Net [3, 19-21];
- архитектура Bot Net [4, 7];
- техническое описание и типы Bot Net [5];

– методы защиты электронных устройство от вредоносного программного обеспечения, способного инфицировать устройство и подключить его к Bot Net [22-26];

– методы выявления и борьбы с Bot Net [6, 9, 18];

Исследование методов и средств защиты персональных страниц от Bot Net является одной из актуальных проблем, отражаемой в книгах и публикациях последних лет. Статья [15] содержит детальное описание методики заражения Bot Net. Особое внимание в работе уделяется указаниям на ошибки пользователя. Автором описаны идеи возможных уязвимостей систем и устройств.

Разбор признаков доказательства наличия инфекции Bot Net на устройстве проведен в работе [16]. Кроме базовых признаков, таких как медленная работа устройства, большая нагрузка процессора, проблемы с доступом в Интернет, рассмотрены и продвинутые методы – проверка сетевых каналов, обнаружение увеличения трафика на определенных портах, проверка соединений с серверами, замеченными в составе различных Bot Net.

Немаловажно сравнение типов Bot Net и выявление недостатков каждого, что призвано классифицировать целевые направления их применения. Этот вопрос рассмотрен в материале [7]: от ранних видов управления ботами и непопулярных, но имеющих место быть, до видов гораздо новее, а также описываются типы использования собственных протоколов.

В работах [22-25] содержится необходимая информация о уязвимостях Bot Net в зависимости от архитектуры Bot Net и типов устройств, что является ключевым в возможности заражения и функционировании Bot Net.

Разные направления применения Bot Net требуют разного подхода к методам исследований и последующей разработки методов защиты. Рассылка спама и создание поискового спама рассмотрены в работах [1, 13]. Проведение DDoS-атак является одним из самых распространенных видов применений Bot Net и рассмотрено в статье [10]. Сбор конфиденциальной информации очень важно предотвратить, потому что вред направлен не только на технические возможности и мощности пользователя, но и на его персональные данные. Этот вопрос детально освещен в работах [11, 12].

Отличительной особенностью обзора [18] является наличие в нем исследования Bot Net и использования систем-приманок, которые имитируют несколько уязвимостей и автоматизирует сбор данных, полезных для понимания угрозы в целом, потенциала и динамики развития. В конечном итоге, результаты этих исследований помогают лучше понять природу Bot Net, но на процесс предотвращения их использования влияют только косвенно.

Идея многоагентной системы защиты описана в статье [9] и представляет из себя кластерную структуру из агентов разных типов, каждый из которых имеет определенную задачу и выделенные функции. Этот метод предоставляет базовую защиту, широко доступен за счет широкого распространения обновляемых исходных данных для каждого кластера, а также, производится обеспечение резервирования. Что немаловажно, метод может эксплуатироваться

как обычными конечными пользователями, так и организациями, заинтересованными в своей защите, в том числе и в сетях провайдеров.

В работах [22-25] рассматривается широкий круг вопросов, связанных с различными методами борьбы персональных страниц пользователя от Bot Net, у каждого из которых разная степень сложности исполнения, а также разные виды распространения и лицензии.

В статье [25] описываются методы предотвращения распространения Bot Net. Рассмотрены применимые действия пользователей и хостинг-провайдерам. Что немаловажно, в случае с хостинг-провайдером защищаемый от DDoS-атаки сайт сохраняет работоспособность.

Рассмотренные материалы несут информацию, необходимую для изучения функционирования Bot Net разных типов и целей, а также их уязвимости, с целью практической реализации защиты персональных страниц пользователя и страниц хостинг-провайдеров от рассмотренных типов и уязвимостей Bot Net до реализации систем-приманок и применения многоагентного метода.

Список литературы

1 Craig A. Schiller, Jim Binkley, David Harley, Gadi Evron, Tony Bradley, Carsten Willems, Michael Cross. Botnets — The Killer Web App. — M. : Syngress, 2007 — C. 29—77 — ISBN-10: 1-59749-135-7.

2 E. Cooke, F. Jahanian, and D. McPherson.The zombie roundup: Understanding, detecting and disrupting botnets. Cambridge, MA, July 2005.

3 Eggdrop: Open Sourse IRC bot. [Электронный ресурс]. – Режим доступа: http://www.eggheads.org/.

4 Ping Wang, Baber Aslam, Cliff C. Zou.Handbook of Information and Communication Security. Peer-to-Peer Botnets — M. Springer — C. 335—350 — ISBN 978-3-642-04116-7.

5 Heron, Simon. Botnet command and control techniques. Network Security. April, 2007.

6 Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, Giovanni Vigna. Your Botnet is My Botnet: Analysis of a Botnet Takeover. November 9—13, 2009, Chicago, Illinois, USA.

7 Paul Barford. An Inside Look at Botnets. University of Wisconsin, Madison.

8 A.C. Atluri, V. Tran. Botnets Threat Analysis and Detection. — M. : Springer, 2017 — C. 15—27.

9 6 Tools to Detect Zombie Bot Malware Infection on Windows Computer. [Электронный ресурс]. – Режим доступа: https://www.raymond.cc/blog/is-your-computer-a-zombie-bot-being-controlled-by-hackers/.

10 The cost of launching a DDoS attack. [Электронный ресурс]. – Режим доступа: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/.

11 Ботнет Великий и Ужасный. Компьютерра Online. [Электронный ресурс]. – Режим доступа: http://old.computerra.ru/focus/317787/.

12 "Ботнеты: беда, откуда не ждали" № 584, июль 2012 г. [Электронный ресурс]. – Режим доступа: https://upweek.ru/botnety-beda-otkuda-ne-zhdali.html.

13 The Spamhaus Project. [Электронный ресурс]. – Режим доступа: https://www.spamhaus.org/statistics/botnet-cc/.

14 How your smart device helped destroy the internet for a day. [Электронный ресурс]. – Режим доступа: http://mashable.com/2016/10/21/dyn-attack-iot-device/.

15 Here Are the Sites You Can't Access Because Someone Took the Internet Down. Fusion. [Электронный ресурс]. – Режим доступа: https://splinternews.com/here-are-the-sites-you-cant-access-because-someone-took-1793863079.

16 150,000 IoT Devices behind the 1Tbps DDoS attack on OVH. [Электронный ресурс]. – Режим доступа: http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html.

17 KrebsOnSecurity Hit With Record DDoS. [Электронный ресурс]. – Режим доступа: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

18 Wenke Lee, Cliff Wang, David Dagon. Botnet Detection. Countering the Largest Security Threat — M. : Springer, 2008 — ISBN-13: 978-0-387-68766-7

19 Ботнеты. Всё о ботнетах. [Электронный ресурс]. – Режим доступа: https://helpugroup.ru/botnety-vse-o-botnetah/.

20 Ботнет. Как создаются ботнеты. Средства защиты от ботнетов. [Электронный ресурс]. – Режим доступа: https://www.windxp.com.ru/articles29.htm.

21 Как построить свой личный ботнет и сколько это стоит. [Электронный ресурс]. – Режим доступа: http://www.computerra.ru/65142/kak-postroit-svoy-lichnyiy-botnet-i-skolko-eto-stoit/.

22 Защита сайта от хакерских атак. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/pentestit/blog/282860/.

23 Защита сайта от DDoS и хакеров. [Электронный ресурс]. – Режим доступа: https://айри.рф/защита_сайта_ddos.

24 Как закрывают ботнеты. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/xakep/blog/130792/.

25 Наносим удар по ddos ботнету своими силами. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/134359/.

26 Ботнет. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Ботнет.

ИСПОЛЬЗОВАНИЕ ИНТЕРАКТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ПОДГОТОВКИ БУДУЩИХ IT-СПЕЦИАЛИСТОВ

Глотова М.И., канд. пед. наук, доцент
Оренбургский государственный университет

В современных условиях развитие высшего образования проходит этап переосмысления в контексте использования образовательных технологий, применяемых в учебном процессе. В условиях экономики информационного общества все большую необходимость приобретает подготовка будущих специалистов, способных быть мобильными в принятии решений, готовых относительно быстро и гибко менять свои профессиональные функции. Процессы информатизации заставляют обратить особое внимание на совершенствование подготовки будущих IT-специалистов, сфера профессиональной деятельности которых критически важна для современного общества [2]. В связи с чем особенно актуальным становится применение интерактивных образовательных технологий в процессе обучения.

Особенностью интерактивных образовательных технологий можно считать их ориентированность на разнообразное взаимодействие не только студентов с преподавателем в конкретной учебной дисциплине, но и студентов разных курсов (проектная деятельность), а также самих преподавателей (межпредметные связи) [1]. Роль интерактивных технологий в образовательном процессе вуза заключается в развитии у студентов умений работать сообща, например, в учебных мини-проектах, во временных командах, малых группах и стремиться к качественным результатам. Использование таких технологий позволяет студентам обогатить свой опыт и добыть через учебную деятельность те компетенции социального взаимодействия, которые затем могут оказаться необходимыми в их будущей профессиональной и социальной жизни.

В целях эффективной подготовки будущих IT-специалистов по направлению 09.03.02 Информационные системы и технологии в нашем исследовании активно применяется метод проектов, ориентированный на самостоятельное планирование и поэтапное выполнение студентами постепенно усложняющихся задач и заданий.

В основу комплекса усложняющихся заданий положена прежде всего прагматическая направленность на результат, который студент может получить при решении той или иной практически или теоретически значимой проблемы. Этот результат можно увидеть, осмыслить, применить в реальной практической деятельности. Для достижения такого результата необходимо научить студентов самостоятельно мыслить, находить и решать проблемы, привлекая для этой цели знания из разных областей, умения прогнозировать результаты и возможные последствия разных вариантов решения.

Комплекс усложняющихся задач и заданий в процессе преподавания дисциплины «Программирование Web-приложений» разрабатывается нами с учетом следующих требований:

– значимость задачи или проблемы (в зависимости от уровня сложности) в исследовательском плане (применение интегрированного знания, комплекса умений, актуализация знаний и умений, полученных при изучении нескольких тем);

– познавательная и практическая значимость (реальная востребованность получаемых результатов);

– самостоятельная работа обучающихся (индивидуальная или в команде).

В содержание дисциплины «Программирование Web-приложений» включены следующие разделы:

1. Основы HTML;
2. Введение в CSS;
3. Основы языка JavaScript;
4. Основы языка PHP.

В рамках каждого раздела дисциплины мы выделяем комплекс усложняющихся задач и заданий, где задания представлены следующими уровнями:

1-уровень - типовые задачи исполнительского характера, направленные на закрепление основных понятий и освоение базовых умений; уровень предполагает решение задачи по ранее изученному алгоритму;

2-уровень - комплексные задания, имеющие формализованный смысл (четкий контекст, требуемый результат), интегрирующие знания, умения и опыт деятельности по использованию понятий, полученных при изучении нескольких тем осваиваемого раздела; уровень характеризуется поисковой активностью, готовит студентов к принятию решений, предполагает способность студента выбрать необходимые, адекватные знания, умения, способы информационной деятельности;

3-й уровень – творческий, представляет собой творческие проекты, имеющие неформализованный смысл, интегрирующие знания, умения, опыт деятельности, полученные при изучении двух и более разделов дисциплины и/или нескольких дисциплин; предполагает нахождение студентом новых идей и способов решения задач; уровень характеризуется креативностью, самостоятельностью в принятии решений.

В рамках всей дисциплины нами предусмотрены проектные задания различных уровней, выполнение которых интегрирует в себе знания, умения, опыт деятельности, полученные при изучении всех разделов, и предполагает разработку стилизованных динамических сайтов, созданных средствами не только языка HTML и каскадных таблиц стилей CSS, но и языков JavaScript и PHP.

Представим примеры формулировок усложняющихся заданий в рамках раздела «Основы JavaScript». Например, в качестве заданий могут быть следующие:

1. Написать сценарий изменения цвета кнопки, например, от синего к голубому и наоборот, т.е. создать визуальный эффект подсветки кнопки, возникающий при наведении (и/или уходе) указателя мыши на изображение кнопки (1 уровень).
2. Написать сценарий, который размещает на странице раскрывающийся список и изображение. При выборе элемента списка должно изменяться изображение. Использовать предварительную загрузку изображений путем создания его объекта в памяти браузера с помощью конструктора (2 уровень).
3. Создайте HTML-страницу содержащую форму для заполнения данных пользователя, которые должны будут отправлены на адрес электронной почты. Следует предусмотреть проверку введенных пользователем данных, например, заполнено ли поле имени, введен ли пароль и совпадают ли значения, введенные в оба поля для паролей, корректен ли введенный электронный адрес и пр. При несоблюдении условий, курсор должен установиться в то поле, где пользователем введено неверное значение. Комплекс проверяемых условий разработать самостоятельно (3 уровень).

Представим формулировки усложняющихся проектных заданий, которые могут быть реализованы как индивидуально, так и в команде:

1. Создать статическую Web-страницу, на которой разместить информацию о себе и будущей выбранной профессии. При создании использовать различные элементы: абзацы и переводы строки, заголовки разных уровней, разделы, списки, элементы логического и физического форматирования, бегущую строку и пр.
2. Создать стилизованный Web-сайт для некоторого общественного заведения. Все страницы Web-сайта должны быть выдержаны в едином стиле (модерн, восточный стиль, классический стиль и т.п.). На страницах Web-сайта необходимо представить перечень мероприятий (развлечений), меню заведения, акции для привлечения посетителей и прочую информацию.
3. Создать Web-сайт «Витрина интернет-магазина» для расчета стоимости заказываемых товаров и услуг. Реализовать вывод предлагаемых товаров и услуг с помощью интерактивных форм. Помимо описания товаров и услуг должна быть представлена их стоимость из прайс-листа. С помощью элементов языков JavaScript и PHP необходимо осуществить расчет стоимости выбранных товаров и услуг, а также реализовать вывод стоимости корзины пользователя на экран. Использовать динамические эффекты.

Таким образом, при выполнении проектного задания 1-го уровня студенты используют только возможности языка разметки гипертекста HTML5. Выполнение проекта 2-го уровня предполагает задействование студентами возможностей каскадных таблиц стилей, для придания своему Web-сайту стилизованного внешнего вида. Проектные работы 3-го уровня включают в себя

создание и внедрение сценариев, позволяющих сделать стилизованный сайт динамическим.

В результате выполнения подобных проектных заданий происходит активное взаимодействие студентов, в котором обучающиеся взаимно обогащаются знаниями, ценностями в области современных информационных технологий, приобретают способы коллективной деятельности в решении проблемных ситуаций, накапливают опыт творческой деятельности, осуществляют рефлексию, через которую устанавливается отношение студента к собственному действию и адекватная коррекция этого действия.

Список литературы

1. Макаренко О.В. Интерактивные образовательные технологии в вузе / О.В. Макаренко // Высшее образование в России. - 2012, № 10. – С. 134-139.

2. Куликова Е.В. Применение методов интерактивного обучения в процессе подготовки будущих IT-специалистов в вузе / Е.В. Куликова // Вестник Сибирского института бизнеса и информационных технологий. - 2014, № 1(9). – С. 70-74.

3. Гулакова М. В., Харченко Г. И. Интерактивные методы обучения в вузе как педагогическая инновация // Научно-методический электронный журнал «Концепт». – 2013. – № 11 (ноябрь). – С. 31–35.

4. Гущин Ю. В. Интерактивные методы обучения в высшей школе // Психологический журнал Международного университета природы, общества и человека «Дубна». – 2012 . – № 2. С. 1 – 18.

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ МАТЕМАТИКИ НА ТЕХНИЧЕСКИХ СПЕЦИАЛЬНОСТЯХ В УНИВЕРСИТЕТСКОМ КОЛЛЕДЖЕ ОГУ

Гурьянов А.А.
Университетский колледж
Оренбургского государственного университета

У абитуриентов, приходящих в колледж или другое среднее специальное учебное заведение, после девятого класса в большинстве случаев недостаточный, а бывает, что и очень низкий, уровень математической подготовки. Главная проблема здесь в том, что учащиеся школ получают слабую математическую подготовку, направленную лишь на то, чтобы выпускники девятых классов прошли основной государственный экзамен (ОГЭ) по математике и успешно отправились покорять светлое будущее. Обучающимся на технических специальностях первого курса тяжело осваивать программу математической подготовки согласно стандартам специальностей СПО.

Математически слабо подготовленному обучающемуся сложно осваивать математику в рамках программ подготовки специалистов среднего звена. Математику на первом курсе изучают в сжатой и интенсивной форме. Поэтому здесь очень важно иметь хорошую базовую математическую подготовку, что бы своевременно осваивать курс математики по выбранной специальности. Кроме того, в средних специальных учебных заведениях, как правило, много часов отводится на самостоятельную работу и это ведет к тому, что количество часов аудиторных занятий по математике, по сравнению со школой, уменьшается. Но бывшие ученики школ, в своем большинстве, не могут самоорганизоваться на самостоятельную работу, у них нет тяги к самообразованию, они тратят время в пустую и, как следствие, наблюдаются пробелы в изучении математики.

Таким образом, важными условиями повышения уровня качества математической подготовки обучающихся технических специальностей среднего профессионального образования является повышенная интенсивность занятий, ориентированность в профессиональное направление аудиторных и внеаудиторных занятий, грамотная организация внеаудиторной самостоятельной работы обучающихся по дисциплине математика. Нехватка учебного времени, при изучении дисциплины математика, на аудиторных занятиях выводит проблему наиболее рационального использования этого времени. Значит, нужно определять повышенные требования к содержанию учебных занятий, их наполнению, профессиональной направленности.

В Университетском колледже ОГУ очень большое внимание уделяют математической подготовке на технических специальностях. Например, обучаясь на втором курсе по специальности 24.02.01 Производство летательных аппаратов студентам кране необходимо знать уметь и владеть математическим аппаратом в области математической статистики. Им приходиться производить расчеты, связанные с выборкой и ее характеристиками. В частности, по дисциплине «Аэродинамика» обучающимся приходиться выполнять

практические работы, в которых есть задания по расчету функции надежности по заданной выборке значений. Таким образом, для того, что бы справиться с выполнением этих заданий, необходимы достаточно хорошие знания в области теории надежности и математической статистики. На занятиях по математике в колледже студентам предлагаются для решения следующие задания: по заданной выборке произвести расчет числовых характеристик, определить эмпирическую функцию распределения вариационного ряда и так далее.

Студенты обучаются производить расчеты по определению геометрических и аэродинамических характеристик летательных аппаратов, учатся строить и анализировать графики основных характеристик летательных аппаратов. Следовательно, чтобы овладеть этими умениями требуются хорошие знания в области геометрии и построении графиков функций. В Университетском колледже большое внимание при изучении математики уделено разделам, связанным с геометрией (параллельность и перпендикулярность в пространстве, декартовые координаты в пространстве, геометрические тела) и построением графиков функций заданных аналитически и таблично.

Обучаясь на специальности 15.02.18 Технология машиностроения студенты, в обязательном порядке, должны владеть техникой геометрических построений. Например, по дисциплине «Инженерная графика» главным умением, которым должны овладеть студенты это выполнение графических изображений технологического оборудования и технологических схем, а также строить чертежи геометрических тел и их проекций. Следовательно, геометрическая подготовка обучающихся крайне важна. Кроме того, практически по всем техническим дисциплинам, обучающимся важно уметь производить различные расчеты с помощью формул (аналитически).

В колледже при изучении разделов геометрии студенты учатся строить геометрические тела и их проекции на плоскость, производить расчеты, связанные с геометрическими телами, например: вычисление объемов и площадей поверхностей геометрических тел (пирамиды, конуса, цилиндра и так далее). Кроме того, серьезное внимание уделяется построению сечений геометрических тел. Студенты выполняют такое задание: построить сечение пирамиды плоскостью проходящей через точки, лежащие на боковых ребрах пирамиды или не ее гранях. Все геометрические построения проводятся с помощью карандаша, линейки, циркуля. Большое внимание уделяется аккуратности построения, точности, соблюдение масштаба.

При изучении разделов связанных с функциями студенты овладевают умениями построения графиков различных функций, заданных аналитически, определение свойств функций (область определения, четность, периодичность, промежутки возрастания и убывания, критические точки и точки экстремума и так далее). Умения построения графиков функций поможет в дальнейшем при изучении дисциплин, в которых необходимо графически изображать различные процессы (например, физические процессы или химические). Кроме того, студенты учатся читать графики функций.

Одной из тем в математическом образовании колледжа, которую студенты изучают с удовольствием, является «Логика высказываний». На специальности 11.02.02 Техническое обслуживание и ремонт радиоэлектронной техники (по отраслям) студенты на занятиях по математике учатся строить релейно-контактные схемы и определять условия работы таких схем. Для того, чтобы это уметь делать необходимо научиться по заданной формуле строить релейно-контактную схему, задавать схему с помощью формулы, уметь строить таблицу истинности по заданной или построенной формуле и по этой таблице правильно определять условия, при которых схема будет проводить ток. В частности студенты выполняют примерно следующие задания: составить релейно-контактную схему, состоящую из четырех контактов, которая будет проводить ток тогда и только тогда, когда любые два контакта разомкнуты.

Рассмотрены выше лишь только некоторые примеры математического образования в Университетском колледже ОГУ. На самом деле при изучении математики рассматривается большое количество тем таких как: производная, вычисление интегралов различными методами (заменой переменной, подведением под знак интеграла, интегрирование по частям), решение дифференциальных уравнений, вычисление интегралов по формулам прямоугольника, трапеции и Симпсона и так далее.

На технических специальностях Университетского колледжа ОГУ математика разделена на две части. Первая часть преподается на первом курсе в течение двух семестров и представляет собой школьный курс математики за десятый и одиннадцатый классы. Вторая часть это элементы высшей математики. Она преподается на втором курсе на всех технических специальностях. В дальнейшем все те знания, которые студент получает на занятиях математики, он будет использовать практически на всех дисциплинах до окончания своего обучения в колледже. В том числе и в выпускной квалификационной работе.

Список литературы

1. Баврин, И. И. Математика для технических колледжей и техникумов : учебник и практикум для спо / И. И. Баврин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2016. — 397 с.- (Профессиональное образование) .- ISBN 978-5-534-08026-1 .- (ЭБС Юрайт) .- Режим доступа : https://biblio-online.ru/viewer/matematika-dlya-tehnicheskih-kolledzhey-i-tehnikumov-424130#page/2 .- Загл. с экрана

2. Погорелов, А.В. Геометрия. Базовый и профильный уровень : учебник для 10 - 11 кл. сред. школы / А.В. Погорелов .– 13-е изд.– М. : Просвещение, 2014 .– 128 с.- ISBN 978-5-0903-2026

МАТЕМАТИЧЕСКИЙ КРУЖОК КАК ФОРМА РАЗВИТИЯ ИНТЕРЕСА ОБУЧАЮЩИХСЯ К МАТЕМАТИКЕ

Колобов А.Н., канд. техн. наук, доцент
Оренбургский государственный педагогический университет

Привлечь внимание детей и вызвать их удивление – это лишь начало возникновения интереса, и добиться этого сравнительно легко; труднее удержать интерес детей к внеклассной работе и дополнительному образованию по математике и сделать его постоянным и устойчивым.

Перечислим некоторые общие положения, которых следует придерживаться при воспитании интереса к математике:

– материал, предлагаемый для изучения должен быть понятен каждому ребенку, иначе он не вызовет интереса;

– на занятиях по математике полезно использовать различные виды наглядности: полную предметную, неполную, символическую, представления по памяти, – исходя из уровня развития мышления учащихся. Особенно умело и вовремя надо использовать детское воображение, которое в данном возрасте ярче и сильнее интеллекта. Поэтому волшебные сказки и мультипликационные герои служат прекрасным средством воспитания и развития детей;

– устойчивый интерес к математике поддерживается тем, что дополнительные математические занятия проводится систематически, а не от случая к случаю. На самих занятиях постоянно должны возникать маленькие и доступные для понимания детей вопросы, загадки, создаваться атмосфера, возбуждающая активную мысль учащихся.

Математический кружок

Занятия могут проводиться по программам одной тематической направленности или комплексным, интегрированным программам. Предусматриваются разные формы проведения занятий: групповые, индивидуальные, со всем составом детского объединения. Для учащихся 10 – 14 лет наиболее распространенной, традиционной и эффективной формой объединения детей по интересам являются кружок.

Кружок способствует формированию и развитию интереса учащихся к математике, расширяет и углубляет математические знания, развивает математический кругозор, мышление, способности, исследовательские умения школьников, позволяет в дальнейшем сделать правильный выбор профессии. Кружки организуются на добровольных началах для всех желающих школьников. Возможно создание кружков с уровнями (для более сильных и средних учащихся); с секциями (учебно-исследовательская, оформительская, любителей решения задач); с определенной тематикой. В состав кружка входит примерно 10 –15 учащихся. На первом занятии следует выбрать старосту, актив и редколлегию кружка. Желательно придумать название, эмблему, девиз. Занятия кружка обычно проводятся 2 – 4 раза в месяц. Продолжительность занятий не должна превышать одного часа. Начинать работу кружка лучше с начала октября, а завершать в конце апреля. Итогом работы кружка может стать математический вечер. План работы кружка обычно составляется на год. Форма плана может быть любая. При планировании работы кружка необходимо

отразить: номер занятия; дату проведения; содержание занятия; фамилии учащихся, ответственных за подготовку; примечания.

Список литературы для подготовки к занятиям кружка:

1. Балк, М.Б. Математика после уроков / М.Б. Балк, Г.Д. Балк. – М.: Просвещение, 1971.

2. Виленкин, Н.Я. Популярная комбинаторика / Н.Я. Виленкин. – М.: Наука, 1975.

3. Гарднер, М. Математические чудеса и тайны / М. Гарднер. – М.: Наука, 1982.

4. Гусев, В.А. Внеклассная работа по математике в 6-8 классах / В.А.Гусев, А.И. Орлов, А.Л. Розенталь. – М.: Просвещение, 1977.

5. Доморяд, А.П. Математические игры и развлечения / А.П. Доморяд. – М., 1961.

6. Дышинский, Е.А. Игротека математического кружка / Е.А. Дышинский. – М.: Просвещение, 1972.

7. Зубелевич, Г.И. Занятия математического кружка в 4 классе / Г.И. Зубелевич. – М.: Просвещение, 1980.

8. Игнатьев, Е.И. В царстве смекалки / Е.И. Игнатьев. – М.: Наука, 1981.

9. Коваленко, В.Г. Дидактические игры на уроках математики / В.Г. Коваленко. – М.: Просвещение, 1990.

10. Кордемский, Б.А. Математическая смекалка / Б.А. Кордемский. – М.: Юнисам, МДС, 1994.

11. . Лоповок, Л.М. Математика на досуге. – М.: Просвещение, 1981.

12. . Математический кружок. Вып. 1, 2. – М.: Бюро-Квантум, 1998.

13. Мерлина, Н.И. Дополнительное математическое образование школьников и современная школа. – М.: Гелиос АРВ, 2000.

14. Нагибин, Ф.Ф. Математическая шкатулка / Ф.Ф. Нагибин, Е.С. Канин. – М., Просвещение, 1988.

15. Перельман, Я.И. Живая математика. – Екатеринбург: Тезис, 1994.

16. Петраков, И.С. Математические кружки в 8–10 классах / И.С. Петраков. М.: Просвещение, 1987.

17. Фарков, А.В. Математические кружки в школе. 5–8 классы. – М.: Айрис-пресс, 2005.

18. . Шуба, М.Ю. Занимательные задания в обучении математике. – М.: Просвещение, 1995.

Основные формы проведения занятий кружка:

1. Комбинированное тематическое занятие – наиболее традиционная форма. Примерная структура занятия: сообщение учителя или учащегося (5–10 минут); решение задач по определенной теме, в том числе задач повышенной трудности; решение задач занимательного характера, задач на смекалку, разбор математических софизмов, фокусов, проведение математических игр, развлечений; моделирование; чтение и обсуждение математических книг и статей; выпуск математического листа или газеты; ответы на вопросы учащихся и многое другое.

2. Занятия-семинары. Участники кружка предварительно разбиваются на группы по 2-3 человека для подготовки выступления по заданной теме. Сообщается план

семинара, назначается председательствующий, который ведет семинар, и два его ассистента, следящие за ходом семинара. Выступающие заранее готовят таблицы, схемы, презентации. К решению задач, выбранных докладчиком для примера, может привлекаться по желанию любой участник кружка. Присутствующие задают вопросы, делятся сомнениями, предлагают новый способ решения. В конце семинара с заключительным словом выступает руководитель кружка (группы, студии), который отмечает самые хорошие доклады, недочеты в ответах, обращает внимание на наиболее «тонкие» места в доказательствах, сообщает тему для следующего обсуждения.

3. Занятия-практикумы проводятся после того, как рассмотрена определенная тема на семинаре. Занятие полностью посвящено решению задач. Учащиеся могут разбиваться на группы для совместного обсуждения и решения задач, а могут решать их индивидуально. У доски разбираются решения только тех задач, которые вызвали затруднения хотя бы у одной группы учащихся. При этом задача полностью не решается, а разбирается до того момента, с которого дальнейший путь ясен. На занятиях-практикумах вполне уместны конкурсные и олимпиадные задачи, решение которых опирается на изучаемый материал

4. Комбинированное занятие разновозрастного кружка .Схема проведения занятия: а) лекция по новой теме (читают два лектора: вузовский преподаватель и школьник – в 1-й группе ученик 7 класса, во 2-й – ученик 10 класса); б) выступление школьников по домашнему заданию (3–4 школьника разных классов с разными заданиями); в) новое домашнее задание к следующему занятию; г) творческое задание, предлагаемое самими школьниками для всей группы или математическая игра с вручением символического приза или досрочного права выдать новое задание участникам группы.

5. Итоговое занятие кружка может быть проведено в форме математического вечера, олимпиады и т.п. Завершить занятие следует обязательным поощрением наиболее отличившихся учащихся; рекомендациями по каникулярному чтению математической литературы; рассмотрением перспектив работы кружка в следующем году. Вечера лучше проводить в форме театрализованного представления. Темами могут быть: «История развития чисел» и др. Формы организации вечера – игры «Что? Где? Когда?», «Звездный час», «Счастливый случай» и др.

Математические игры и развлечения.

Одним из древнейших средств воспитания, обучения и развития учащихся считается игра. Включение игры в учебный процесс заметно повышает интерес к учебному предмету, создает ситуации, наполненные эмоциональными переживаниями, стимулирует деятельность учащихся. В игре осуществляется личностное становление школьников.

Структурные элементы игры: установочный элемент, игровая ситуация, задачи игры, игровые правила, игровое действие, игровое состояние, результат игры.

Начало любой игры осуществляется вместе с созданием у учащихся эмоциональной установки на игру. Установочный элемент игры – это своеобразная предигровая ситуация, обеспечивающая организационные предпосылки на восприятие игровых задач, создающая познавательную мотивацию, активизирующая мыслительную деятельность, воображение школьников. Установка на игру обычно создается в увлекательной форме, иногда с использованием слайдов, рисунков,

кинофрагментов. Установочный элемент игры позволяет ввести школьников в игровую ситуацию. В игровой ситуации участвует определенное количество учащихся, которые реализуют определенные действия. Следующим структурным элементом игры являются игровые задачи. Большинство исследователей выделяют как игровые, так и учебные задачи. Учебные задачи выступают для учащихся в замаскированном, неявном виде. Благодаря учебным задачам осуществляется непреднамеренное обучение школьников. Игровая задача заинтересовывает школьников (реши кроссворд, найди ошибку и т.д.). Отсутствие в игре игровой задачи превращает ее в обычное задание, упражнение. Для соединения учебных и игровых задач необходимы правила игры. Они организуют поведение учащихся, обеспечивают игрокам равные условия. Игровые правила реализуются в игровых действиях. Чем разнообразнее действия, тем интереснее игра. Основные требования к игровым действиям учащихся: игровые действия должны быть мотивированы, спланированы и управляемы, должны соответствовать числу играющих и постепенно усложняться. Во время игры у учащихся возникает игровое состояние. Оно включает в себя наличие переживания, активизацию воображения учащихся, эмоциональное отношение к действительности. Игровое состояние поддерживают проблемность ситуации, элементы соревновательности и занимательности, используемые аксессуары, наличие юмора, элементов дискуссии, свободная творческая атмосфера, ситуация выбора. Обязательным структурным элементом игры является ее результат. Результат может быть наглядным (выиграл, отгадал, выполнил), менее заметным (получил удовлетворение, заинтересовался вопросом) и отсроченным (создал свой вариант игры через определенное время). Различают результат для учителя, заключающийся в показателе уровня усвоения знаний и умений, норм поведения, и для учащихся – в достижении определенных целей (моральное удовлетворение от игры, отгадывание кроссворда, интерес к проблеме). Игры классифицируют по различным признакам: игры с правилами (настольные; игры-состязания; подвижные игры на местности; компьютерные) и творческие игры (ролевые; игровое проектирование; компьютерные) в зависимости от творческой активности учащихся

Общий смысл развития мотивации учения состоит в том, что учителям желательно переводить учащихся с уровней отрицательного и безразличного отношения к учению к зрелым формам положительного отношения к учению — действенному, осознанному и ответственному.

Список литературы

1 Колобов, А.Н. Оценка значимости математико-экономических задач в образовании. / А.Н. Колобов / «Университетский комплекс как региональный центр образования, науки и культуры»: материалы Всероссийской научно-методической конференции – Оренбург: Оренбургский государственный университет, 2018. – с. 1818-1821.

2 Колобов, А.Н. Разработка компетентностно-ориентированных задач и возможные их применения в преподавании математических дисциплин. / А.Н. Колобов, И.В. Прояева / «Современные проблемы физико-математических наук»: материалы IV Всероссийской научно-практической конференции с международным участием – Орёл: ОГУ имени И.С. Тургенева, 2018.–с.116-119.

РОЛЬ ТЕКСТОВЫХ ЗАДАЧ В МАТЕМАТИЧЕСКОМ ОБРАЗОВАНИИ

Колобов А.Н., канд. техн. наук, доцент
Оренбургский государственный педагогический университет

Математика является простором и свободой для размышления. Она очень важна в процессе взаимодействия со многими областями деятельности людей, и это оказало огромное влияние на развитие науки в целом.

Одним из показателей, указывающим на математическое развитие человека является умение работать с текстовой задачей. С первого дня поступления ребёнка в школу происходит знакомство с математическими задачами. На протяжении всей школьной жизни учащиеся сталкиваются и решают текстовые задачи. При тесном взаимодействии задачи непрерывно помогают школьникам вырабатывать основные математические термины и понятия, позволяют глубже окунуться во взаимодействие с окружающим миром, показывают применение изучаемых теоретических положений на практике. Текстовые задачи это не только объект познания, ознакомления и образования конкретных навыков и умений, также они являются средством становления математических понятий. Текстовые задачи есть основной инструмент обучения математике. Педагоги и методисты считают, задания, направленные на решение задач приводят у ребят к образованию отрицательных эмоций. Многие ребята, даже не приступают к решению задач в контрольных вариантах и на экзамене. Поэтому решению текстовых задач отведена значительная роль, потому что данные задачи позволяют развивать у школьников логику мышления, память, речь, внимание. Однако нельзя не отметить и существование того, что нередко у школьников возникает любопытство к процессу нахождения плана решения, при достижении которого ребята получают душевную удовлетворенность.

Текстовые задачи – достаточно нелёгкий и замысловатый материал для большого круга школьников. Они связывают теорию с практикой, направлены на совершенствование у учащихся математического мышления, вырабатывают на практике навыки применения понятий и определений, служат инструментом развития пространственного воображения. Они способствуют формированию у ребят важных для жизни знаний, а на их базе – умений и навыков, направленных на решение проблемных ситуаций.

Становление и образование у ребят умений и навыков решения текстовых задач – это одно из существенных решений методики преподавания математики. Встречаясь с данными задачами, учащиеся убеждаются на практике, что элементарные математические понятия имеют огромное значение в будничной жизни людей. Во многих книгах есть описание системы приёмов, способных облегчить поиск способа решения задач, но теоретические положения мало разработаны и применены на практике [1].

Ведущие ученые России, такие как: Г. В. Дорофеев, И. И. Зубарева, А.Г. Мордкович отмечают: «Школьный курс математики способствует становлению общего развития у ученика, созреванию нравственных качеств личности».

Сообщество не работающих в школе учителями математики психологов предложили учащимся решить задачу: «На плоскости даны пять точек, являющиеся вершинами пятиугольника. Проведите карандашом четыре отрезка так, чтобы зачеркнуть все точки, и не отрывая карандаш от бумаги, вернитесь в исходную точку». Более 500 ребят не решили эту задачу. Другой же психолог, работавший ранее учителем математики, проделал этот эксперимент и с тем же результатом. Но когда он задал всего лишь один - единственный вопрос: «Какая фигура получится в итоге (как выглядит конечный результат)?» - почти все ответили правильно.

Этот вопрос не является сложным. Учащимся необходимо было задать себе этот вопрос. Но они не знали ни этого, ни других наводящих вопросов. Не знали даже, с чего начать, так как обычно в школе действовали по шаблону и не учатся поиску решения задачи.

Для того чтобы прийти к правильному решению задачи нужно её прочитать, устно сформулировать, создать математический образец решаемого вопроса, определить тип задачи, выбрать метод и способ решения.

Учащиеся знакомятся со многими фактами окружающего мира при чтении задач. Существуют разнообразные способы решения математических задач. Подбор наиболее рационального способа решения задачи показывает уровень математической обученности школьников. Имеет большое значение научить каждого школьника работать с задачей в широком смысле этого слова.

Каждая математическая задача направлена на достижение педагогической, учебной, дидактической цели, а формулировки этих целей показывают содержание самой задачи. На уроке следует применять различные способы и методы решения текстовых задач. Из-за взаимодействия различных методов и средств обучения школьники могут глубже окунуться в тему, более сознательно усвоить учебную информацию.

Задачи - это одна из существенных форм учебного действия в процессе постижения математики, а также средство математического процветания ребёнка. Правильно организованный процесс обучения решению задач может быть эффективным средством общего развития ребёнка.

Математика вызывает больший интерес у тех учеников, которые умеют решать задачки. Научив каждого ребенка решать текстовые задачи, мы вычеркнем из урока и жизни его нехорошие эмоции, и это вызовет у него заинтересованность к предмету математики.

С первой ступени обучения в школе происходит работа по становлению способности решать текстовые задачи. Решение простых задач как правило не вызывает у учащихся затруднений. Однако впоследствии индивидуально решить задачу практически не по силам многим ученикам, и от класса к классу эти учащиеся испытывают внушительные препятствия.

Причина данных затруднений: не сформирован опыт чтения и анализа текста задачи, определение известного и неизвестного, выявление их взаимосвязей, которые служат фундаментом выбора действия для решения задачи.

Текстовые задачи имеют большое значение в математике. Умение решать текстовые задачи показывает уровень состояния образования. Если учитель будет

понимать смысл текстовой задачи, ее структуру, знать различные способы решения данных задач, то у его учащихся при решении текстовых задач будет развиваться мышление, внимание, память, речь. Решая текстовые задачи школьники и усваивают новые математические определения, и применяют эти знания на практике [2].

«Задача – это то, что требует разрешения, исполнения» - толковый словарь русского языка С. И. Ожегова.

«Задача – это цель деятельности, которая задана в определенных условиях и требует для своего использования приемлемых этим условиям средств» - психологический словарь.

В математике принято понимать: каждая текстовая задача – это ориентир в проблемных ситуациях.

Под задачей в широком смысле понимают проблемную ситуацию с заданной целью, которую необходимо достичь. В узком смысле понятие задача определяется как цель, то есть то, что требуется сделать.

Известный психолог Л. М. Фридман считает, что: «Задача – это некоторое требование или вопрос, на который необходимо ответить, опираясь на те условия, которые заданы в задаче».

Педагоги – математики, считают что текстовую задачу нужно понимать как проблемную ситуацию (вопрос), которую необходимо решить используя математические умения и навыки.

Что значит решить задачу? Необходима умственная деятельность, направленная на достижение поставленных целей. Чтобы решить задачу, нужно проанализировать ситуацию, выявить определенную последовательность действий, при использовании которых получаем ответ на вопрос задачи. Только разобрав, поняв и изучив задачу, выяснив взаимосвязь между компонентами, можно приступать к ее решению.

Каждая математическая текстовая задача – это выразительный, логично построенный рассказ, в котором есть известные и неизвестные величины, находящиеся в зависимости друг от друга, с указанными условиями.

В каждой текстовой задаче есть взаимосвязь между условием и ее целью. Каждая задача состоит из условия и цели. Если отсутствует один из компонентов, то и самой задачи нет. Чтобы решить текстовую задачу нужно определить методы ее решения. Для того чтобы провести анализ текстовой задачи, нужно установить связь между условием задачи и соотнести с вопросом данной задачи.

Каждая текстовая задача представляет собой некоторую определенную ситуацию, правило. Решение может быть:

- приобретение новых знаний (например, решение задачи на отыскание части от целого числа);
- итоговое положение (например, сбор развёртки параллелепипеда);
- образование отношений между компонентами (например, необходимость выяснить, какая скорость больше).

Каждая текстовая задача направлена на выполнение одной из четырёх функций:

- для обучающей функции характерно становление структуры математических знаний, умений и навыков;

- для воспитывающей функции характерно воспитание у школьников заинтересованности к математике;

- для развивающей функции характерно развитие мышления ребят;

- для контролирующей функции характерно обозначение степени усваивания учебной информации, возможности их к индивидуальному усвоению школьного материала.

Все математические задачи разделены на простые и составные по числу действий.

Простая задача – это задача, в которой необходимо выполнить одно действие.

Задача 1. У фермера в хозяйстве 3 га заняты усадьбой, под посевами 380 га. Сколько всего земли в пользовании у фермера?

Составная задача – это задача, в которой необходимо выполнить несколько действий.

Задача 2. В магазин привезли морковь, которая была продана за три дня. В первый день продали 448 кг моркови, что составило 28% всей моркови. Во второй день продали 45% остальной моркови. Сколько килограммов моркови продали в третий день?

При решении простых задач у учащихся формируется понятие об арифметических действиях. Простые задачи – это подготовительный этап перед решением составных задач. Решая простые задачи учащиеся знакомятся с задачами и их составными частями.

Составная же задача включает в себя несколько простых, связанных между собой задач, где искомые одних простых задач являются данными для других. Разделив составную задачу на ряд простых задач – процесс решения составных задач. Таким образом, чтобы решить составную задач необходимо установить взаимозависимость искомых и данных.

Любая текстовая задача состоит из условия (то, что дано) и требования (вопрос задачи).

Условие характеризуется сообщением об объектах и известных и неизвестных величинах, дающих характеристику объектам, об известных и неизвестных значениях величин, о взаимосвязи этих объектов.

Требование характеризуется указанием. В нем сообщается то, что необходимо найти.

Задача 3. Вес космонавта на Луне равен 12 кг, что составляет 16% веса этого же космонавта на Земле. Сколько будет весить космонавт на Земле?

В данной задаче три неизвестных величины, одна из которых заключена в требовании задачи. Эта величина называется искомой.

Задача 4. Мастер может изготовить 360 деталей за 6 дней, а ученик – за 12 дней. За сколько дней мастер и ученик смогут изготовить это количество деталей, работая одновременно?

В данной задаче пять неизвестных величины, одна из которых заключена в требовании задачи.

Иногда встречаются задачи, где часть условия или всё условие заключено в одно предложение с требованием задачи.

Задача 5. Чему равен объём прямоугольного параллелепипеда, длина которого 0,3 м, ширина 36 см, а высота 2,5 дм?

Каждая текстовая задача содержит следующие элементы:

- словесное изложение текста задачи, которая содержит в себе взаимосвязь между известными и неизвестными величинами;
- числовые значения величин, о которых идёт речь в задаче.

Современная литература разделяет задачи по:

1) характеру вопроса:
- задачи на доказательство;
- задачи на построение;
- задачи на вычисление.

2) функциональное предназначение:
- дидактическая функция;
- познавательная функция;
- развивающая функция.

3) по количеству проблем:
- стандартные (все компоненты известны);
- обучающие (неизвестен один компонентов из пяти);
- поисковые (неизвестны два компонента из пяти);
- проблемные (неизвестны три, четыре компонента из пяти).

Также бывают задачи стандартного и нестандартного вида, теоретические и практические, устные и письменные и т.д.

Текстовые задачи занимают важное место в жизни каждого школьника. Решая задачу, учитель должен осознанно подходить к выбору и подбору, должен четко понимать, какое действие может оказать каждая задача на обучение и воспитание школьника.

Правильно поставленная математическая задача раскрывает традиционную и современную методику преподавания. Задачи можно применять при изучении новой темы, для проверки знаний, так как они направляют школьников на поисковую, творческую деятельность.

Так как задача – это проблемная ситуация, которая требует решение, то ее роль в обучении очень важна. При решении текстовых задач у школьников вырабатывается умение ориентироваться в новых ситуациях, собирать необходимую информацию для решения некоторых заданий.

Список литературы

1 Колобов, А.Н. О задачах на построение в школьных учебниках геометрии в России в XVIII веке. / А.Н. Колобов, И.В. Прояева / История науки и техники. Научный журнал. - 2018 г.- № 7. - с.43-47.

2 Колобов, А.Н. Разработка компетентностно-ориентированных задач и возможные их применения в преподавании математических дисциплин. / А.Н. Колобов, И.В. Прояева / «Современные проблемы физико-математических наук»: материалы IV Всероссийской научно-практической конференции с международным участием – Орёл: ОГУ имени И.С. Тургенева, 2018. – с. 116-119.

ФАКУЛЬТАТИВНЫЕ КУРСЫ ПО МАТЕМАТИКЕ КАК ФОРМА РАЗВИТИЯ МАТЕМАТИЧЕСКИХ СПОСОБНОСТЕЙ

Колобов А.Н., канд. техн. наук, доцент
Оренбургский государственный педагогический университет

Планируя систему внеклассной работы в современной школе, необходимо учитывать закономерности развития учебной деятельности, связанные с возрастными особенностями школьников, в соответствии с которыми и должен осуществляться выбор содержания и форм внеклассной работы. Следует помнить и о вариативности и личностной направленности содержания в профильной подготовке и профильном обучении. При планировании внеклассной работы методическому объединению учителей математики желательно обозначать не только, какие мероприятия будут проведены, но и цели, ответственных за подготовку и проведение мероприятий.

Внешкольная работа по математике, в отличие от внеклассной, которая проводится с учащимися одной школы учителями математики (а иногда и родителями учащихся) этой же школы, организуется с учащимися нескольких школ региона. Внешкольная работа предназначена для учащихся, увлеченных математикой. Основные цели организации внешкольной работы: развитие мышления и математических способностей учащихся; углубление знаний учащихся по математике. Основные формы внешкольной работы по математике: математические кружки и факультативы при вузах, Домах творчества, Центрах дополнительного образования; летние математические школы; математические соревнования между школами, городами; районные и городские научные конференции школьников. Проводят внешкольную работу, как правило, преподаватели и студенты вузов, Домов творчества, а также и учителя некоторых школ. Внешкольные занятия с учащимися могут организовываться на базе школы, вуза, Центра дополнительного образования, Дома творчества и т.д.

Для включения школьников в дополнительное образование необходим определённый уровень сформированности интереса к соответствующему виду деятельности. Он достигается как раз при систематическом участии детей во внеклассной работе по математике [1].

Наиболее распространенные формы, с помощью которых возможна реализация дополнительного математического образования школьников: 1) традиционные (математические спецкурсы, кружки, факультативы; математические игры, соревнования, конкурсы, олимпиады; математические экскурсии; математическая печать, математические вечера, недели (декады) математики; чтение математической литературы; различные формы углубленной специальной математической подготовки, реализуемой в очно-заочных, заочных, каникулярных математических школах и лагерях и т.д.); 2) нестандартные (математические конференции; математические общества учащихся; научно-исследовательская работа; проектная деятельность

школьников; разнообразные дистанционные формы дополнительного математического образования школьников и т.д.).

Факультативные курсы по математике являются основной формой внеклассной работы. Главными целями этих занятий являются расширение, углубление знаний в области математики, развитие интереса учащихся к предмету, развитие математических способностей, а также воспитание некоторых навыков самостоятельной работы. У учащихся есть большое стремление проверить свои способности в математике, научиться решать нестандартные задачи.

Факультативные занятия помогают в выборе профессии ориентации учащихся в области математики, облегчая выбор профессии и последующее совершенствование в ней.

Программа основного курса математики параллельно с программой факультативных занятий по математике в школе составляет программу повышенного уровня для учащихся.

Программа факультативных занятий по математике составлена так, что все её темы могут изучаться одновременно с изучением основного курса математики. Иногда изучение некоторых тем факультатива может проводиться независимо от основного курса программы.

Главная задача факультативных курсов – это пробуждение у школьников потребности активно мыслить, преодолевать трудности при решении всевозможных задач, находить оптимальные их пути решения. Научить их доказывать существование вводимых математических понятий, опровергать ложные высказывания, проверять правильность обратного высказывания и т.д.

Так же факультативные занятия готовят учащихся к математическим олимпиадам, выступлениям на математических вечерах. Таким образом, факультативы положительно влияют на внеклассную работу.

Для достижения результатов факультативы должны быть организованы там, где есть высоко квалифицированные педагоги, которые будут проводить занятия на высоком уровне, а также должно быть не менее 15 учащихся, стремящиеся заниматься математикой.

Запись учащихся на факультативные занятия происходит добровольно в соответствии с их интересами. Не нужно заставлять учащихся изучать факультативные предметы. В завершении курса учащиеся сдают зачет с оценкой.

Факультативные занятия по математике должны быть для учащихся интересными и увлекательными. Нужно использовать естественную любознательность ученика для развития устойчивой заинтересованности к своему предмету.

Основными формами проведения факультативов являются лекции семинары, дискуссии, решение задач, рефераты, доклады учащихся и так далее. Но преподавателю не стоит отдавать предпочтение той или иной форме или методу изложения. Нужно не забывать о том, что на факультативах по математике самостоятельная работа школьников должно занять основное

положение, необходимо ставить в приоритет решение задач, рефераты, доклады, дискуссии и т.п.

Каждое занятие курса можно разделить на 2 части. Первая часть включает изучение нового материала и самостоятельной работе учащихся по заданиям теоретического характера. В конце этой части занятия учащимся даётся домашнее задание по изучению темы. Вторая часть занятия посвящена решению наиболее интересных задач и задач повышенной трудности.

На факультативном занятии необходимо уделять внимание развитию следующих умений и навыков:

- умению слушать объяснение нового материала, вести конспект занятий;
- умению работать с учебником по математике;
- умению написать реферат на определённую тему;
- умению подготовить доклад или сообщение по прочитанному материалу;
- умению решать задачи, доказывать теоремы, определённые программой факультатива.

Содержание факультативного курса «Дуальные числа»

Тема «Дуальные числа» формирует и углубляет заложенные в основном курсе математики представления о числах, в известном смысле завершая курс формирования понятия числа в средней школе.

Факультативный курс по «Дуальным числам» рассчитан для учеников 11 классов школ с углубленным изучением математики.

Изучение данной темы рассматривает следующие основные цели:

1) повышение математической культуры учащихся;
2) углубление представлений о понятии числа;
3) дальнейшее развитие представлений о единстве математики как науки.

К теме «Дуальные числа» относятся такие задачи, решение которых можно получить, не выходя за рамки поля действительных чисел, с помощью весьма искусственных индивидуальных приемов и хитроумных рассуждений. Решение таких задач с применением дуальных чисел оказывается очень простым и естественным.

Содержание темы изложено в трёх параграфах:

§1 «Множество дуальных чисел»;

§2 «Модуль и аргумент дуального числа»;

§3 «Геометрическое изображение дуального числа».

В первом параграфе вводится определение дуальных чисел и действий над ними. Дуальные числа вводятся как формальные выражения вида $a + b\varepsilon$, где a и b – действительные числа.

Второй параграф содержит понятия модуля и аргумента дуального числа, так же в нем вводятся формулы возведения в степень и извлечения корня дуальных чисел.

В третьем параграфе рассматривается геометрическая интерпретация дуальных чисел и формулы расстояния между точками и угла между прямыми.

На факультатив по дуальным числам отводится 14 часов. Примерное распределение часов приводится ниже.

§1. «Множество дуальных чисел» - 4 часа;

§2. «Модуль и аргумент дуального числа» - 5 часа;

§3. «Геометрическое изображение дуального числа» - 3 часа.

Всего 12 часов. Из оставшихся двух часов один лучше всего использовать для контрольной работы, а второй для разбора контрольной и устного опроса тех, кто с ней не справился.

В конце изучения факультативного курса по дуальным числам учащиеся должны научиться выполнять действия над дуальными числами, пользоваться геометрическими изображениями дуального числа и геометрической интерпретацией действий над дуальными числами, применять формулы возведения дуального числа в степень и извлечения корней из дуальных чисел [2].

С 2004 г. Министерство образования и науки РФ ввело в 10–11 классах элективные курсы. Элективные курсы – это обязательные для посещения курсы по выбору учащихся, входящие в состав профиля обучения. Число элективных курсов предлагается больше, чем число курсов, которые должны выбрать учащиеся. Ясно, что тематика элективных курсов может быть тесно связана с планом всей внеклассной работы по математике.

Содержание факультативных курсов в 7–9 классах должно быть практико-ориентированным и занимательным. В 10–11 классах содержание должно быть направлено на подготовку учащихся к продолжению образования.

Существуют специальные, рекомендованные МО РФ программы по факультативным занятиям.

Для учащихся 7–9 классов – программа «За страницами учебника математики» с приложением «Математическая мозаика».

В качестве одного из возможных факультативных курсов по углубленному изучению математики в 10–11 классах МО РФ предложило «Подготовительный факультатив», основной целью которого являлась подготовка учащихся к поступлению в вуз. Факультативный курс может проводиться по авторской программе.

Список литературы

1 Колобов, А.Н. О задачах на построение в школьных учебниках геометрии в России в XVIII веке. / А.Н. Колобов, И.В. Прояева / История науки и техники. Научный журнал. - 2018 г.- № 7. - с.43-47.

2 Колобов, А.Н. Математические задачи с экономическим содержанием в современном образовании. /А.Н. Колобов/ «Университетский комплекс как

региональный центр образования, науки и культуры»: материалы Всероссийской научно-методической конференции – Оренбург: Оренбургский государственный университет, 2018. – с. 1812-1817.

ИСПОЛЬЗОВАНИЕ ДИАГРАММ ДЕЯТЕЛЬНОСТЕЙ В ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ

Кузниченко М.А.
Орский гуманитарно-технологический институт (филиал) ОГУ

В настоящее время система образования в России находится под давлением возрастающего объема требований как со стороны общества, так и государства, относительно качества и интенсивности подготовки специалистов разных профессиональных квалификаций. Новый подход государства предполагает создание единого образовательного пространства на всей территории Российской Федерации и его интеграцию в общеевропейскую систему образования. На это направлены реформы, проводимые министерством образования РФ, внедрение в учебный процесс федеральных образовательных стандартов по инженерным направлениям бакалавриата, компетентностный подход в учебном процессе.

Следует отметить важную роль развития аналитических способностей студентов при проектировании и реинженеринге информационных систем в их будущей профессиональной деятельности. Для успешной разработки информационной системы (ИС) объект проектирования должен быть прежде всего адекватно описан, то есть должны быть построены полные и непротиворечивые модели архитектуры ПО, обусловливающей совокупность структурных элементов системы и связей между ними, поведение элементов системы в процессе их взаимодействия, а также иерархию подсистем, объединяющих её структурные элементы. Язык моделирования UML обладает широким спектром диаграмм для достижения этой цели. Именно поэтому изучение языка UML позволяет формировать у будущих специалистов профессиональные навыки в области проектирования ИС.

Построение моделей в языке UML можно представить как некоторый процесс поэтапного спуска от абстрактной концептуальной модели исходной системы к логической, а затем и к физической модели программной системы. На начальном этапе проектирования, как правило, строятся диаграммы вариантов использования (use case diagram), которые выявляют субъекты системы и описывают её функциональное назначение. На следующем этапе проектирования ИС целесообразно выполнить построение диаграммы деятельностей (activity diagram) для каждого варианта использования.

В отличие от большинства других средств UML диаграммы дея-тельностей основаны на нескольких различных методах, в частности методе моделирования состояний SDL и сетях Петри. Эти диаграммы особенно полезны в описании поведения, включающего большое количество параллельных процессов. Диаграммы деятельности позволяют моделировать сложный жизненный цикл объекта, с переходами из одного состояния в другое. Данный вид диаграмм может быть использован и для описания динамики совокупности объектов.

Диаграмма деятельностей предоставляет разработчику свободу выбора порядка выполнения действий. Другими словами, она только устанавливает основные правила последовательности, которым необходимо следовать. Такая возможность важна при моделировании бизнес-процессов. Среди бизнес-процессов нередко встречаются такие, которые не обязаны выполняться последовательно. В таких ситуациях данный метод хорошо работает, так как он позволяет реализовывать процессы параллельно.

Если при описании поведения системы имеются параллельные деятельности, то их необходимо синхронизировать, для этого используется линейка синхронизации. Простая линейка синхронизации показывает, что её выходная деятельность активизируется только тогда, когда выполнены обе входные деятельности.

На диаграмме деятельности отображается логика и последовательность переходов от одной деятельности к другой, а внимание аналитика фокусируется на результатах. Результат деятельности может привести к изменению состояния системы или возвращению некоторого значения.

Основными компонентами диаграммы деятельности являются начало, конец, процесс или действие, линейка синхронизации и ветвление с указанием состояний объекта (рисунок 1).

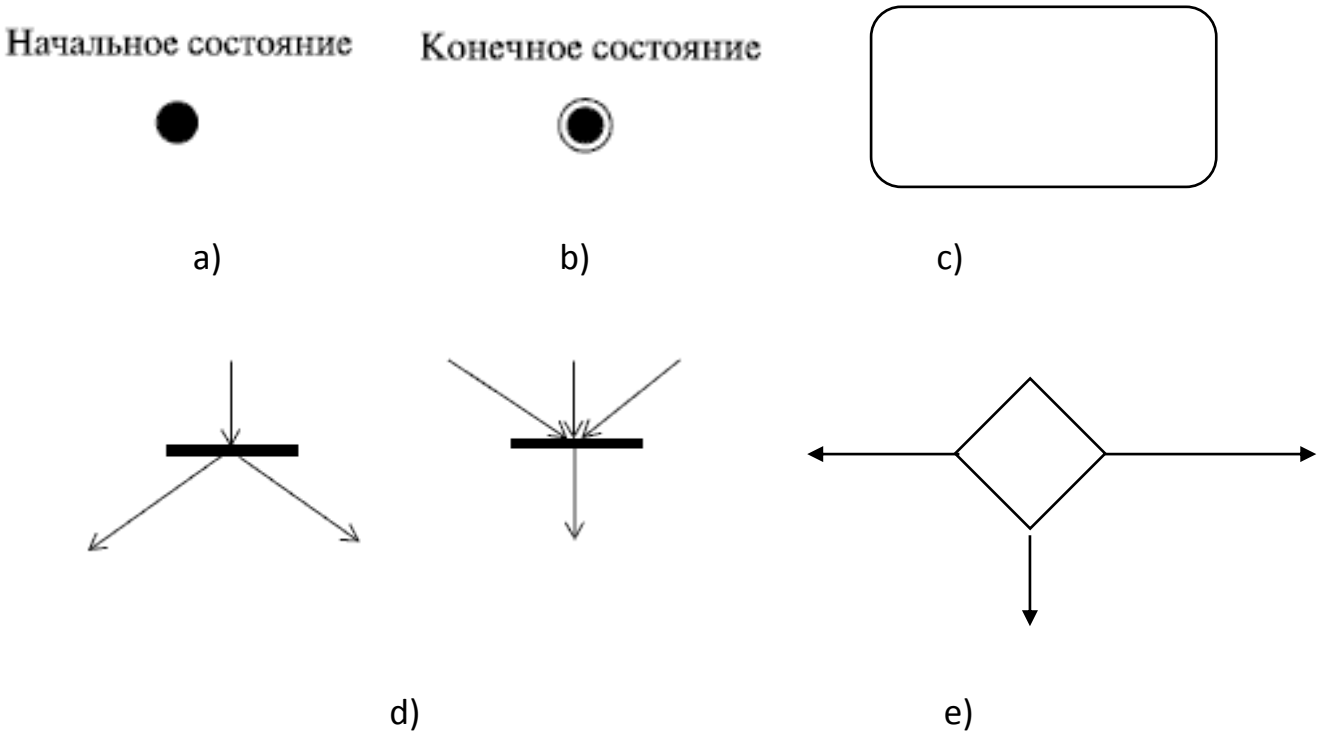


Рисунок 1 – Компоненты диаграммы: a) начало; b) конец; c) действие d)линейка синхронизации; e) ветвление

В качестве примера описания деятельности можно рассмотреть авторизацию пользователя в некоторой системе. Для начала работы в ИС пользователю, как правило, необходимо пройти авторизацию путём ввода логина и пароля. При корректном вводе данных, откроется главное меню

программы, при неверном вводе данных система выдаст ошибку и будет ожидать повторного ввода данных. На диаграммах активности можно использовать «дорожки», распределяющие деятельности в соответствии с ролями (объектами), их выполняющими.

На рисунке 1 показана диаграмма деятельностей входа пользователя в систему. На диаграмме выделены два объекта: пользователь и система, которые инициируют определённые действия.

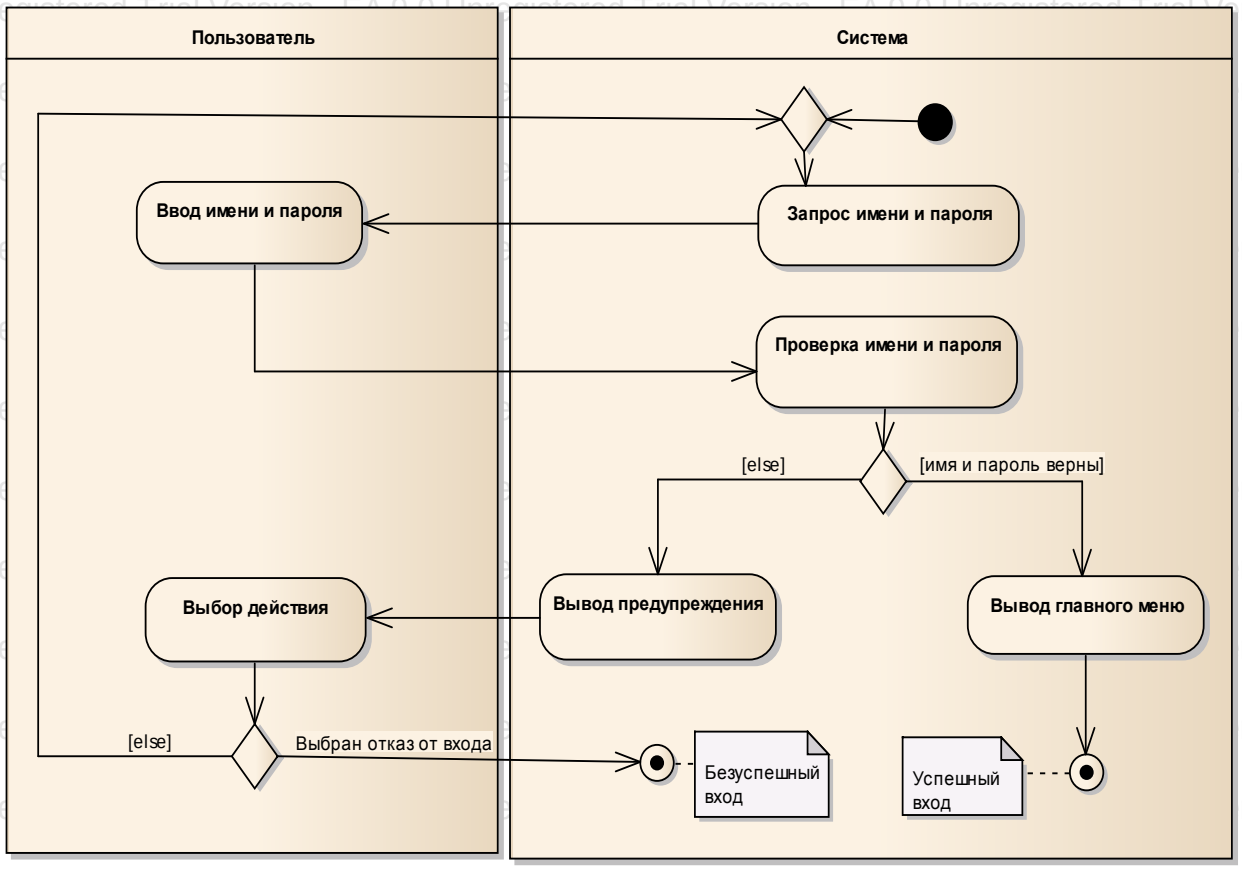


Рисунок 1 – Диаграмма деятельности авторизации пользователя

Другой пример иллюстрирует деятельность, которую инициирует пользователь при выполнении запроса к базе данных. В этом процессе участвуют три объекта: клиент, веб- сервер и сервер базы данных. После отправки запроса клиента веб- сервер анализирует его права на получение данных и запрещает или разрешает данное действие. Собственно выборка данных выполняется на стороне сервера баз данных, а пользователю передаются результаты запроса. На рисунке 2 показана диаграмма деятельности выполнения запроса к базе данных.

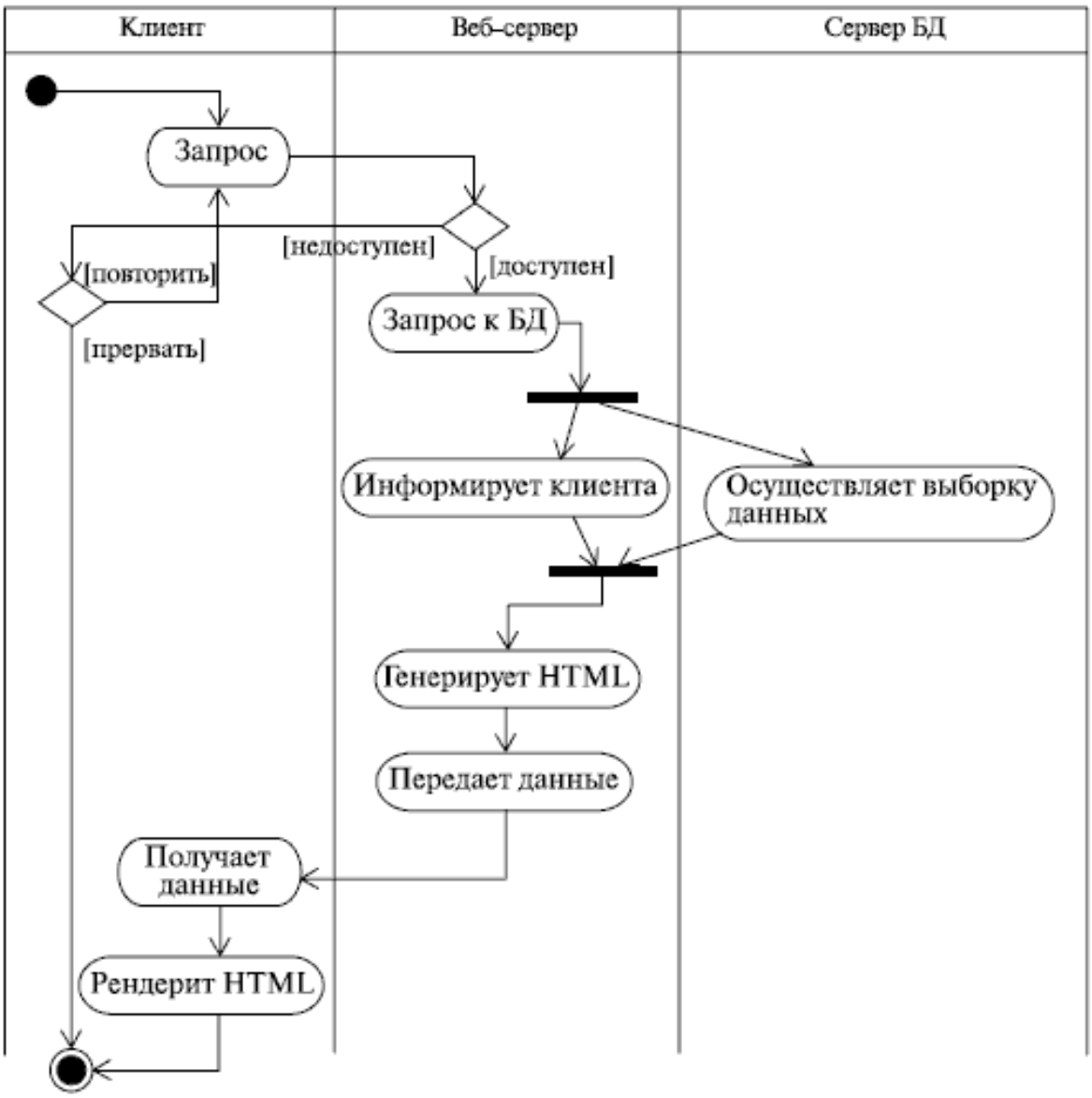


Рисунок 2 – Диаграмма деятельности запроса к базе данных

Диаграммы деятельности лишь моделируют срез некоторых динамических аспектов поведения системы. С помощью единственной диаграммы деятельности никогда не удастся охватить все динамические аспекты системы. Следует использовать разные диаграммы деятельности для моделирования динамики рабочих процессов или отдельных операций.

Таким образом, диаграммой деятельности можно дополнить любой элемент модели, имеющий динамическое поведение. Диаграммы деятельности являются частным случаем диаграммы состояний. В отличие от блок-схем, диаграммы деятельности могут отображать одновременно выполняемые действия. Так же на диаграммах активности можно использовать «дорожки», распределяющие деятельности в соответствии с ролями (объектами), их выполняющими. Траектория объекта позволяет показать объекты, относящиеся к деятельности, и моменты переходов этих объектов из одного состояния в другое. Сложные деятельности можно дополнительно детализировать, разбив на

действия и изобразив "диаграмму в диаграмме". Диаграммы деятельностей можно использовать для проектирования бизнес-процессов или вычислительных операций.

Построение различных диаграмм используется при изучении таких дисциплин как «Проектирование информационных систем», «Технология разработки программного обеспечения», «Конструирование программного обеспечения» и других.

Список литературы

1. Проектирование программного обеспечения экономических информационных систем: Учебник. - 2-е изд., перераб. и доп. Автор: Вендров А.М. Издательство: М.: Финансы и статистика, 2006.- 544с., ISBN: 5-279-02937-83.

2. Ларман К. Применение UML 2.0 и шаблонов проектирования. Введение в объектно- ориентированный анализ, проектирование и итеративную разработку. – США: «Вильямс», 2013. – 736 с.

МАСШТАБИРОВАНИЕ ОБЛАЧНЫХ СЕРВИСОВ ДЛЯ МУЛЬТИОБЛАЧНОГО ЦЕНТРА КОЛЛЕКТИВНОГО ДОСТУПА

Полежаев П.Н., Легашев Л.В.
Оренбургский государственный университет

Повышение эффективности функционирования мультиоблачных систем коллективного доступа напрямую связано с разработкой алгоритмов эффективного масштабирования ресурсов используемых облачных сервисов. Задача масштабирования Web-приложений, вычислительных и DaaS (Desktop as a Service) сервисов в облачной среде является актуальной, что подчёркивается многими исследованиями на указанную тематику.

В публикации [1] представлена новая архитектура и алгоритм для динамического масштабирования web-приложений на основе пороговых значений активных сессий. Предложенное авторами исследования решение способно обрабатывать внезапные скачки нагрузки, предоставлять конечным пользователям информационные ресурсы по требованию, сокращая при этом затраты на инфраструктуру и управление. Работа [2] посвящена описанию основных принципов работы интегрированной среды облачных вычислений InterCloud, которая обеспечивает своевременную масштабируемость облачных сервисов, а также соблюдение требований QoS (Quality of Service) в условиях переменной нагрузки, ресурсов и сетевых условий. Ученые из Имперского колледжа Лондона в своем исследовании [3] представили интеллектуальную платформу для управления виртуальными ресурсами облачных приложений, включая масштабирование на уровне виртуальных машин и более детальное масштабирование на уровне ресурсов (процессора, оперативной памяти, I/O и т.д.). При разработке алгоритмов авторы оперируют понятием стоимости потребления ресурсов и эксплуатационными расходами облачных провайдеров; двумя пороговыми значениями по предельному использованию центрального процессора и оперативной памяти, а также требованиями QoS к верхней и нижней границе времени отклика, приемлемой для пользователей в рамках соглашения об уровне услуг SLA (Service Level Agreement). В публикации [4] представлена система CloudScale гибкого масштабирования ресурсов для многопользовательских облачных вычислительных инфраструктур. Система CloudScale использует онлайн-прогнозирование спроса на ресурсы и обработку ошибок прогнозирования с целью достижения адаптивного распределения ресурсов. CloudScale разрешает вопросы конфликтов масштабирования между приложениями с использованием миграции, а также интегрирует динамическое масштабирование напряжения и частоты процессора с целью достижения экономии энергопотребления. Исследователи Xiao Z., Chen Q. и Luo H. В своей работе [5] представляют систему для автоматического масштабирования интернет-приложений в облачной среде. Авторы инкапсулируют каждый экземпляр приложения внутри виртуальной машины и используют технологию виртуализации для обеспечения изоляции ошибок.

Ранее в рамках проводимого исследования нами разработаны модели мультиоблачного центра коллективного доступа. Рассмотрим часть его структурной модели, имеющую значение для задачи масштабирования облачных сервисов. Каждый виртуальный ЦОД, находящийся в составе мультиоблачного центра коллективного доступа, может быть формализован в виде следующего вектора:

$$VDataCenter_i = (VMPools_i, Services_i, Images_i, Provider_i),$$

где $VMPools_i = \{VMPool_{ij}\}_{j=\overline{1,L_i}}$ – пулы виртуальных машин, используемых для назначения сервисов, $Services_i = \{Service_{ij}\}_{j=\overline{1,G_i}}$ – облачные сервисы, запущенные в виртуальном ЦОД, $Images_i = \{Image_{ij}\}_{j=\overline{1,H_i}}$ – дисковые образы виртуальных машин, $Provider_i$ – провайдер, на базе которого развернут виртуальный ЦОД.

Каждый провайдер облачных услуг $Provider_i$ формализуется в виде вектора:

$$Provider_i = (VMTemplates_i, RunCost_i, StoreCost_i, InNetCost_i, OutNetCost_i),$$

где $VMTemplates_i = \{VMTemplate_{ij}\}_{j=\overline{1,D_i}}$ – множество шаблонов виртуальных машин, $RunCost_i : VMTemplates_i \to R^+$ – стоимость выполнения в минуту виртуальной машины, созданной на основе заданного шаблона, $StoreCost_i : Images_i \to R^+$ – стоимость хранения ее дискового образа, $InNetCost_i : VMTemplates_i \to R^+$ и $OutNetCost_i : VMTemplates_i \to R^+$ – соответственно стоимости входящего и исходящего трафика за мегабайт. Учет стоимостных показателей позволит по ним формализовать оптимизационные задачи планирования, масштабирования и миграции сервисов.

Шаблон виртуальной машины $VMTemplate_{ij}$ описывается следующим кортежем:

$$VMTemplate_{ij} = (NCores_{ij}, Frequency_{ij}, SpeedFactor_{ij}, RAM_{ij}, MaxBandwidth_{ij}^{Temp}),$$

где $NCores_{ij} \in N$ – количество вычислительных ядер, $Frequency_{ij} \in N$ – частота ядра в мегагерцах, $SpeedFactor_{ij} \in R$ – относительная производительность вычислительных ядер в пересчете на один мегагерц, $RAM_{ij} \in N$ – размер оперативной памяти в мегабайтах, $MaxBandwidth_{ij}^{Temp} \in R^+$ – максимальная пропускная способность в мегабитах в секунду.

Вычислительная производительность виртуальной машины, запущенной по шаблону $VMTemplate_{ij}$ может быть определена по формуле:

$$Performance(VMTemplate_{ij}) = NCores_{ij} \cdot Frequency_{ij} \cdot SpeedFactor_{ij}.$$

Формализуем шаблон виртуальной машины $ServiceTemplate_i$ следующим образом:

$$ServiceTemplate_i = (ServiceType_i, VMTemplate_i, Image_i),$$

где $ServiceType_i \in \{'DaaS','SaaS','CaaS'\}$ – тип сервиса (DaaS, SaaS – Software as a Service, CaaS – Computations as a Service), $VMTemplate_i$ – используемый тип шаблона виртуальной машины, $Image_i$ – используемый дисковый образ.

Далее рассмотрим подробнее параметры виртуального ЦОД $VDataCenter_i$. Пул виртуальных машин $VMPool_{ij}$ – это группа виртуальных машин $VMs_{ij} = \{VM_{ijk}\}_k$, построенных на базе одних и тех же шаблона ($VMTemplate_{ij} \in VMTemplate_i$) и дискового образа ($Image_{ij} \in Images_i$), используемая для назначения одних и тех же сервисов:

$$VMPool_{ij} = (VMs_{ij}, VMTemplate_{ij}, Image_{ij}).$$

Служба $Service_{ij}$ характеризуется вектором:

$$Service_{ij} = (Instances_{ij}, ServiceTemplate_{ij}, InpRequests_{ij}(t)),$$

где $Instances_{ij} = \{Instance_{ijk}\}_k$ – запущенные экземпляры сервиса, $ServiceTemplate_{ij}$ – шаблон сервиса, $InpRequests_{ij}(t)$ – поток входящих запросов к сервису, появившихся к моменту времени t. Каждый экземпляр сервиса $Instance_{ijk} = (VM_{ijk})$ характеризуется назначенной виртуальной машиной VM_{ijk}, при этом сам экземпляр сервиса может запускаться как непосредственно на виртуальной машине, так и внутри контейнера, который запущен на ней.

Дисковый образ $Image_{ij}$ описывается кортежем:

$$Image_{ij} = (HDD_{ij}, ImageType_{ij}),$$

где $HDD_{ij} \in N$ – размер жесткого диска в мегабайтах, $ImageType_{ij}$ – тип дискового образа. Все дисковые образы заранее подготовлены и содержат все необходимые программы, библиотеки и конфигурации.

Задача масштабирования облачных сервисов $Service_{ij}$ включает в себя решение следующих проблем:

а) Необходимость прогнозирования количества сессий (пользователей) и потребления ресурсов виртуальных машин в пределах определенного временного горизонта, равного времени запуска виртуальных машин $T_{VM.Start}$. Запуск любой виртуальной машины требует время на: ожидание запроса в очереди, создание виртуальной машины, ее загрузку, запуск служб сервиса. В реальности этот показатель составляет 10-15 минут, поэтому масштабирование облачных сервисов не может осуществляться мгновенно и требует прогнозирования вперед показателей, по которым осуществляется масштабирование.

б) Необходимость адекватного подбора количества используемых экземпляров виртуальных машин под каждый сервис. Данная проблема связана с тем, что при недостаточном количестве виртуальных машин пользователи могут получить нарушения SLA: снижение времени отклика (например, для сервиса DaaS) или увеличение продолжительности обработки запросов (например, для

SaaS и CaaS) из-за нехватки оперативной памяти, ресурсов процессоров или каналов связи используемых виртуальных машин. В то же время, при избыточном количестве виртуальных машин возникает проблема их простоя и увеличения расходов на оплату провайдерам за их использование.

в) Многоцелевая оптимизация – нужно одновременно минимизировать стоимость работы сервисов и степень нарушений SLA.

г) Сложность живой миграции ряда сервисов – это, в первую очередь, касается сервисов DaaS, т.к. они используются пользователями в интерактивном режиме. Для сервисов SaaS и CaaS миграция реализуется более просто.

д) Отсутствие устойчивости – быстрое изменение требований к ресурсам в разные моменты времени. Необходимо, чтобы масштабирование имело инерционный эффект, обеспечивающий требуемую устойчивость.

В рамках данной статьи рассмотрим решение проблем а), б), г) и д).

Для каждой службы $Service_{ij}$, в первую очередь, необходимо уметь прогнозировать $N(t, Service_{ij})$ – количество сессий пользователей, которые будут ею пользоваться в момент времени $t \in [T_{current}, T_{current} + T_{VM.Start}]$ (здесь $T_{current}$ соответствует текущему моменту времени). В качестве единиц времени используются минуты, при необходимости, за одну единицу можно принять более длинные временные интервалы, например, 10 минут, 15 минут или 1 час. Для этой цели предлагается использовать сети LSTM (Long Short Term Memory – долгой краткосрочной памяти), которые хорошо себя зарекомендовали в области прогнозирования временных рядов [6]. LSTM является разновидностью рекуррентных нейронных сетей. В данной работе предлагается использовать классические LSTM-ячейки, объединенные в блоки, причем скрытое состояние, вычисленное для одного пакета обучающих данных, используется для инициализации скрытого состояния при обработке следующего пакета. Прогнозирование осуществляется на основе известных данных скользящего окна ширины W – известных векторов данных:

$$(N(T_{current} - W + 1, Service_{ij}), N(T_{current} - W + 2, Service_{ij}), ..., N(T_{current}, Service_{ij})).$$

Помимо количества сессий, сети LSTM могут быть использованы для одновременного прогнозирования агрегированных показателей потребления ресурсов:

а) $TPerformance(t, Service_{ij})$ – требуемая суммарная вычислительная производительность виртуальных машин сервиса для обслуживания запросов пользователей в момент времени t;

б) $TRAM(t, Service_{ij})$ – требуемый суммарный объем памяти в момент времени t;

в) $TBandwidth(t, Service_{ij})$ – требуемая суммарная пропускная способность всех каналов связи в момент времени t.

Наличие данных показателей позволяет определить более точно количество виртуальных машин конфигурации $VMTemplate_{ij}$, которые потребуются для работы сервиса $Service_{ij}$ в момент времени t:

$$M(t, Service_{ij}) = \max\{\left\lceil \frac{TPerformance(t, Service_{ij})}{Performance(VMTemplate_{ij})} \cdot (1 + \delta_{Perf.}) \right\rceil, \left\lceil \frac{TRAM(t, Service_{ij})}{RAM_{ij}} \cdot (1 + \delta_{RAM}) \right\rceil, \left\lceil \frac{TBandwidth(t, Service_{ij})}{MaxBandwidth_{ij}^{Temp}} \cdot (1 + \delta_{Band.}) \right\rceil\}, \quad (1)$$

где $\delta_{Perf.}, \delta_{RAM}, \delta_{Band.} \in [0,1]$ – настраиваемые параметры, задающие дополнительный запас по свободным соответствующим ресурсам процессора, оперативной памяти и каналов связи на случай возможной перегрузки (подбираются экспериментальным путем).

Формализуем алгоритм масштабирования количества ресурсов сервиса $Service_{ij}$:

Шаг 1. Получить текущее время $T_{current}$, присвоить $T_{pred.} = T_{current} + T_{VM.Start}$.

Шаг 2. С помощью сетей LSTM вычислить значения $TPerformance(T_{pred.}, Service_{ij})$, $TRAM(T_{pred.}, Service_{ij})$ и $TBandwidth(T_{pred.}, Service_{ij})$.

Шаг 3. Вычислить количество требуемых виртуальных машин $M(T_{pred.}, Service_{ij})$.

Шаг 4. Проверяется следующее условие:

$$|Instances_{ij}| + NStarted_{ij}(T_{pred.}, Service_{ij}) - NStopped(T_{pred.}, Service_{ij}) < M(T_{pred.}, Service_{ij}),$$

если оно истинное, то инициируем запуск $K(T_{pred.}, Service_{ij})$ машин:

$$K(T_{pred.}, Service_{ij}) = M(T_{pred.}, Service_{ij}) - |Instances_{ij}| - NStarted_{ij}(T_{pred.}, Service_{ij}) + NStopped(T_{pred.}, Service_{ij})$$

и обнуляем счетчик $Scale_down_counter = 0$.

Шаг 5. Проверяется условие:

$$|Instances_{ij}| + NStarted_{ij}(T_{pred.}, Service_{ij}) - NStopped(T_{pred.}, Service_{ij}) > M(T_{pred.}, Service_{ij}),$$

если оно истинное, то:

шаг 5.1. увеличиваем счетчик количества срабатываний таких проверок $Scale_down_counter = Scale_down_counter + 1$;

шаг 5.2. если $Scale_down_counter > Scale_limit$, то:

шаг 5.2.1. выбрать все свободные виртуальные машины, инициировать их остановку и удаление;

шаг 5.2.2. обнулить счетчик $Scale_down_counter = 0$.

Шаг 6. Если условия шагов 4 и 5 ложные, то обнулить счетчик $Scale_down_counter = 0$.

В данном алгоритме использованы следующие дополнительные обозначения:

а) $T_{pred.}$ – время, для которого строится прогноз;

б) $NStarted_{ij}(T_{pred.}, Service_{ij})$ – количество виртуальных машин службы $Service_{ij}$, запуск которых инициирован, и которые будут запущены к моменту времени $T_{pred.}$;

в) $NStopped(T_{pred.}, Service_{ij})$ – количество виртуальных машин службы $Service_{ij}$, остановка которых инициирована;

г) $Scale_down_counter$ – счетчик количества срабатываний условия для уменьшения количества виртуальных машин;

д) $Scale_limit$ - порог количества срабатываний условия для уменьшения количества виртуальных машин.

Данный алгоритм вызывается периодически через единичные интервалы времени. Также возможна модификация данного алгоритма с целью обеспечения большей гибкости при масштабировании, например, когда условие шага 4 (для увеличения количества виртуальных машин) делается менее жестким и допускает некоторое нарушение на несколько виртуальных машин. Такое допустимо, т.к. у ресурсов виртуальных машин может быть задан дополнительный запас через параметры $\delta_{Perf.}, \delta_{RAM}, \delta_{Band.}$, и это в свою очередь обеспечит устойчивость алгоритма. Также может быть изменен шаг 5.2.1, на котором дополнительно инициируется миграция на другие виртуальные машины уже запущенных задач по обработке запросов пользователей (при условии, что запущенный сервис поддерживает такую возможность). Миграция осуществляется с тех виртуальных машин, которые имеют наименьшую загрузку ресурсов.

Предложенный алгоритм масштабирования облачных сервисов реализован в рамках симулятора мультиоблачного центра коллективного доступа. Предварительная его апробация показывает преимущество над стандартными пороговыми алгоритмами масштабирования, которые используют только текущие показатели ресурсов без прогнозирования. Планируется реализация модификаций данного алгоритма и проведение экспериментального сравнения с другими разработками в данной сфере, полученные результаты будут опубликованы.

Работа выполнена при поддержке РФФИ (проекты №18-37-00460 и №18-07-01446).

Список литературы

1. Chieu T. C. et al. Dynamic scaling of web applications in a virtualized cloud computing environment // E-Business Engineering, 2009. ICEBE'09. IEEE International Conference on. – IEEE – 2009. – P. 281-286.

2. Buyya R., Ranjan R., Calheiros R. N. Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services // International Conference on Algorithms and Architectures for Parallel Processing. – Springer, Berlin, Heidelberg – 2010. – P. 13-31.

3. Han R. et al. Lightweight resource scaling for cloud applications // Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012). – IEEE Computer Society – 2012. – P. 644-651.

4. Shen Z. et al. Cloudscale: elastic resource scaling for multi-tenant cloud systems // Proceedings of the 2nd ACM Symposium on Cloud Computing. – ACM – 2011. – P. 1-14.

5. Xiao Z., Chen Q., Luo H. Automatic scaling of internet applications for cloud computing services // IEEE Transactions on Computers. – 2014. – V. 63. – №. 5. – P. 1111-1123.

6. Jozefowicz R., Zaremba W., Sutskever I. An empirical exploration of recurrent network architectures //International Conference on Machine Learning. – 2015. – С. 2342-2350.

ПРИМЕНЕНИЕ БАЛЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЫ КАК ФАКТОР ПОВЫШЕНИЯ МОТИВАЦИИ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ ПРИ ИЗУЧЕНИИ МАТЕМАТИКИ

Максименко Н.В.
Оренбургский государственный университет

Классическая система контроля знаний, умений и навыков студентов осуществляется два раза в год в период экзаменационных сессий. При этом пятибалльная система контроля не может объективно оценить истинные учебные достижения учащегося. Традиционная форма экзамена зачастую неэффективна, поскольку количество получаемой информации с каждым годом растет. На экзамене у преподавателя часто нет возможности проверить знания студента за весь учебный год, вследствие чего происходит усреднение результатов. Данная система не мотивирует учащегося интенсивно трудиться во время межсессионного периода. Балльно-рейтинговая система оценки знаний студентов свободна от недостатков старой, пятибалльной системы. В настоящее время во многих вузах страны активно вводится балльно-рейтинговая система оценки знаний студентов.

На сегодняшний день проблема рейтинга остается открытой. Как подсчитывать рейтинг? Что принять за основу? Как интерпретировать полученные результаты? В связи с этим предпринимается большое количество попыток освоения данной проблемы и решения накопившихся вопросов.

Одним из главных компонентов в высшем образовании является оценка знаний учащихся. Ее результаты оказывают огромное влияние на мотивацию к обучению и будущую карьеру студентов. Кроме того, оценка дает возможность получить важную для вузов информацию о результативности обучения. Поэтому важно осуществлять оценочный процесс профессионально, с учётом накопленных знаний в рассматриваемой сфере. Одной из технологий оценки качества усвоения учебного материала является балльно-рейтинговая система.

Рейтинг (с английского rating) – это отметка, некоторая численная характеристика какого-либо качественного понятия. Рейтинговая система – совокупность правил, методических указаний и соответствующего математического аппарата, реализованного в программном комплексе, обеспечивающего обработку информации как по количественным, так и по качественным показателям индивидуальной учебной деятельности студентов, позволяющего присвоить персональный рейтинг (интегральную оценку, число) каждому учащемуся в разрезе любой учебной дисциплины, любого вида занятий, а также обобщенно по ряду дисциплин. Обычно под рейтингом понимается «накопленная отметка» как по отдельным учебным предметам, так и по циклу дисциплин за определенный период обучения. Принят и такой термин – индивидуальный, кумулятивный индекс (т.е. индекс по сумме отметок).

В практике вузов рейтинг – это определенное численное значение, выражающееся чаще всего по многобалльной шкале (например, 100-балльной) и

интегрально характеризующее успеваемость и знания студента по одной или нескольким дисциплинам на протяжении какого-то промежутка обучения (семестр, год и т.д.)

В своей совокупности рейтинг делится на различные виды, которые регулируют порядок изучения учебного предмета и отметку его усвоения. В том числе:

1) рейтинг по предмету, отражающий текущую работу студента и его результаты на зачете (экзамене);

2) совокупный семестровый рейтинг, который учитывает успеваемость обучаемого по всем дисциплинам, изучаемым в данном семестре;

3) заключительный рейтинг за курс схожих предметов, изучаемых в течение определенного периода;

4) интегральный рейтинг за какой-то период обучения, учитывающий успеваемость студента в целом в течение определенного промежутка обучения.

Цель балльно-рейтинговой системы заключается в создании условий для мотивации самостоятельности учащихся с помощью методов своевременной и регулярной оценки результатов их деятельности в соответствии с реальными достижениями.

Во главе рейтинговой системы контроля знаний находится ряд мотивационных стимулов, среди которых – актуальная и систематическая оценка результатов в точном соответствии с истинными достижениями учащихся, система поощрения хорошо успевающих студентов.

Основные этапы рейтинговой системы контроля знаний:

1) весь курс обучения по предмету разбивается на разделы по темам, контроль по которым обязателен;

2) по окончании обучения по каждому разделу проводится достаточно полный контроль знаний учащихся с оценкой в баллах;

3) в конце обучения подсчитывается сумма набранных баллов за весь период и выставляется общая оценка. Студенты, имеющие итоговую сумму баллов по рейтингу от 86% до 100%, могут быть освобождены от зачетов (экзаменов).

Рейтинговая система контроля знаний не требует какого-либо радикального преобразования учебного процесса, хорошо сочетается с занятиями в системе технологий личностно-ориентированного обучения.

Основная сложность при внедрении рейтинговой системы контроля – заметное увеличение времени подготовки преподавателя к занятиям. Однако с получением опыта острота данного вопроса снижается.

В Оренбургском государственном университете применяется модульная система. Уже с первого курса студентам знакомы критерии оценки модуля. Модули проходят на 8 и 14 неделе обучения. Балльно-рейтинговая система удачно накладывается на такую организацию учебного процесса, при этом активизирует самостоятельную работу студентов, стимулирует творческий подход учащихся к выполнению заданий. В ходе обучения так же используется дифференцированный подход с выделением разноуровневых задач. В ходе

применения балльно-рейтинговой системы в процессе обучения студенты получают объективную оценку успеваемости. В практике вузов рейтинг – это некоторое численное значение, которое выражается в баллах и характеризует успеваемость обучаемого, его компетентность, самостоятельность, творческий подход, участие в научной работе.

По эффективности работы в семестре усвоение учебной дисциплины оценивается максимум в 100 рейтинговых баллов, которые распределяются по формам занятий в зависимости от их весомости и трудоемкости. По итогам текущей работы по предмету в течение семестра учащийся может набрать не более 70 баллов. На конечный контроль отводится 30 баллов.

Распределение баллов по видам учебных работ (теоретический материал, лабораторные работы, практические занятия, курсовое проектирование, индивидуальные домашние задания, контрольные работы и др.) определяется преподавателем, ведущим ту или иную дисциплину. Перевод баллов в пятибалльную шкалу производится следующим образом: 85-100 баллов – «отлично», 71-84 балла – «хорошо», 60-70 баллов – «удовлетворительно», менее 60 баллов – «неудовлетворительно». При набранной общей сумме баллов менее 40 по результатам третьей аттестации студент не допускается к итоговой аттестации по учебному предмету.

При изучении дисциплины «Математика» мною используется балльно-рейтинговая система (таблица 1,2,3).

Таблица 1 – Балльно-рейтинговая система изучения дисциплины «Математика»

п/п	Контролируемые мероприятия	Рейтинговый балл
	2	3
1-8 учебные недели		
	Опрос	10
	Контрольная работа	10
	Всего баллов	**20**
9-14 учебные недели		
	Опрос	10
	Контрольная работа	10
Всего баллов		**20**
15-18 (или иная последняя неделя семестра**) учебные недели**		
	Опрос	10
	Тестирование	20
Всего баллов		**30**
	Промежуточный контроль (указать вид)	**30**
	Выполнение лабораторных работ	10
	Расчетно-графическое задание	10

	Доклад	10
Итого баллов		**100**

Таблица 2 – Шкала перевода баллов в их числовые эквиваленты

Оценка ECTS		
Название	Сумма баллов	Числовой эквивалент
отлично	91 – 100	5
очень хорошо	84 – 90	4
хорошо	74 – 83	4
Удовлетвори тельно	68 – 73	3
посредственно	61 – 67	3
неудовлетворитель но	0 – 60	2

Таблица 3 – Шкала итоговых оценок успеваемости по дисциплинам, завершающимся зачетом

Набранные баллы	0-60	61-100
Зачет-незачет	Незачет	Зачет

Применение балльно-рейтинговой системы выявило основные преимущества и недостатки ее использования (таблица 4).

Таблица 4 – Достоинства и недостатки использования балльно-рейтинговой системы

Преимущества	Недостатки
Регулярность контроля и наглядность результата	Существенная потеря баллов в результате болезни, или других пропусков по уважительной причине
Активизация учебной деятельности студентов	Из-за большого количества студентов в учебных группах не все могут набрать достаточное количество баллов
Стимулирование самостоятельной работы, повышение мотивации студентов	Вероятны межличностные конфликты среди студентов
Прозрачность и возросшая объективность оценивания	Увеличение объема документации и трудоемкости контроля

Введение новых форм контроля и заданий, в том числе для самостоятельной работы студентов	Изменение структуры учебной нагрузки преподавателей, в частности увеличение внеаудиторной работы
Способствует систематической работе студентов	Отсутствие у студентов навыков работы по самостоятельному овладению знаниями, низкий уровень ответственности и самодисциплины
Снижение нагрузки на студентов и преподавателей во время сессии	-
Оперативный контроль знаний	-
Улучшение посещаемости занятий, укрепление дисциплины	-
Организация регулярной обратной связи, что позволяет своевременно определять проблемы обучаемых и корректировать их деятельность в течение семестра, а не во время сессии	-
Обеспечение дифференцированного подхода к студентам и индивидуальная работа с каждым из них	-

Применение балльно-рейтинговой системы повышает мотивацию студентов при освоении образовательных программ, активизирует повседневную систематическую работу по изучению дисциплин, стимулирует их самостоятельную работу, формирует навыки самоорганизации учебного труда и самооценки.

Внедрение балльно-рейтинговой системы накладывает определенные требования и к преподавателям соответствующих учебных предметов. Необходимый для изучения материал должен быть структурирован таким образом, чтобы при соблюдении общей логической последовательности и непрерывности изучения самой дисциплины, он распадался на отдельные блоки (разделы, темы), позволяющие «осуществлять контроль приобретенных студентами знаний, умений и опыта деятельности». Контроль результатов усвоения соответствующих блоков (разделов, тем) должен быть регулярным, оперативным, объективным и открытым, что требует разработки специальных оценочных средств и методов оценивания. Кроме того, должно быть предусмотрено наличие оперативной связи между педагогом и студентами, которая позволяла бы учащимся получать информацию о результатах обучения и ответы на возникающие вопросы, а преподавателю регламентировать процесс обучения и вводить необходимые изменения как содержательного, так и организационного характера.

Список литературы

1. Максименко, Н.В. Проблемы актуализации мотивации академических достижений студентов как факторы повышения качества обучения в университете [Электронный ресурс] / Н.В. Максименко // Вестник ОГУ. – 2018. – №6 (218). – С. 40-46. Режим доступа: http://vestnik.osu.ru/2018_6/7.pdf

2. Ольховая, Т.А. Актуальные задачи модернизации образовательной деятельности регионального университета [Электронный ресурс] / Т.А. Ольховая, С.В. Панкова // Высшее образование в России. – 2018. – Т. 27, № 10. – С. 108-114. Режим доступа: http://vovr.elpub.ru/jour/article/view/1501/1203

АКТУАЛЬНЫЕ ПРОБЛЕМЫ АВТОМАТИЗАЦИИ АДМИНИСТРИРОВАНИЯ СЕТЕВОГО ОБОРУДОВАНИЯ С УЧЕТОМ НАГРУЗКИ ВИРТУАЛЬНЫХ СЕРВЕРОВ

Мельников А.Е., Тагирова Л.Ф., канд. пед. наук, доцент
Оренбургский государственный университет

Сегодня в мире миллионы компьютеров, 80 % которых (и даже больше) объединены в разнообразные информационно-вычислительные сети. Система персональных компьютеров, расположенных на определенной территории и связанных между собой для совместного использования данных, аппаратных компонентов, программ, информации называется компьютерной сетью [1].

Существует несколько причин мировой тенденции к объединению компьютеров в сети: быстрый обмен информацией, передача и получение сообщений, не вставая с места (E-mail, факс, виртуальные конференций и т. д), возможность мгновенно получить любую информацию из любого места на земном шаре, информационный обмен между ПК разных компаний-производителей, которые работают на разном программном обеспечении.

Среди компьютерных сетей есть деление на локальные (Locate Area Network - LAN), глобальные (Wide Area Network - WAN) и региональные. Первый вид охватывает территорию, где расстояние между компьютерами составляет не более 10 километров. Такая сеть используется в пределах одного здания (учреждения). Глобальная сеть охватывает целую страну или даже несколько стран (10 000 км). Региональные сети применяются в пределах района, города.

Любое современное предприятие использует компьютеры и другие устройства коммуникации. Для эффективной организации и функционирования бизнеса компьютеры как раз и объединяются в сеть. Но порой может нарушаться стабильность работы сети, поэтому необходимо своевременное техническое обслуживание компьютерных сетей. Таким образом и возникает сетевое администрирование [2].

Сетевое администрирование подразумевает поддержание в рабочем состоянии оборудования, из которого состоит корпоративная сеть, выявление проблем, препятствующих эффективному использованию ЛВС, и их устранение.

Управление сетью – целенаправленное воздействие на сеть, осуществляемое для организации её функционирования по заданной программе. Оно включает следующие процедуры:

- включение и отключение системы, каналов передачи данных, терминалов;
- диагностика неисправностей;
- сбор статистики;
- подготовка отчётов и тому подобное.

С точки зрения модели OSI управление сетью подразделяется на управление:

- конфигурацией;

- отказами;
- безопасностью;
- трафиком;
- учётом.

Традиционные методы управления основаны на использовании правил. Они предписывают системе управления в компьютерной сети предпринимать определённые действия (например, выдать предупреждающее сообщение на управляющую консоль) при наступлении определённых событий (превышение интенсивностью трафика заранее определённого порогового значения и др.).

Сетевое администрирование возникает, когда у администратора сети появляется потребность и возможность оперировать единым представлением сети, как правило, это относится к сетям со сложной архитектурой. При этом осуществляется переход от управления функционированием отдельных устройств к анализу трафика в отдельных участках сети, управлению её логической конфигурацией и конкретными рабочими параметрами, причём все эти операции целесообразно выполнять с одной управляющей консоли.

Администратор сети должен выполнять следующие задачи:

- Планирование системы;
- Установка и конфигурация аппаратных устройств;
- Установка программного обеспечения;
- Установка сети;
- Архивирование (резервное копирование) информации;
- Создание и управление пользователями;
- Установка и контроль защиты;
- Мониторинг производительности.

Мониторинг сетевого оборудования – процесс постоянного наблюдения за сетевым оборудованием с целью своевременного обнаружения неисправностей и замедления работы сети.

На рисунке 1 представлены результаты мониторинга в компании ОАО «Оренбургоблгаз».

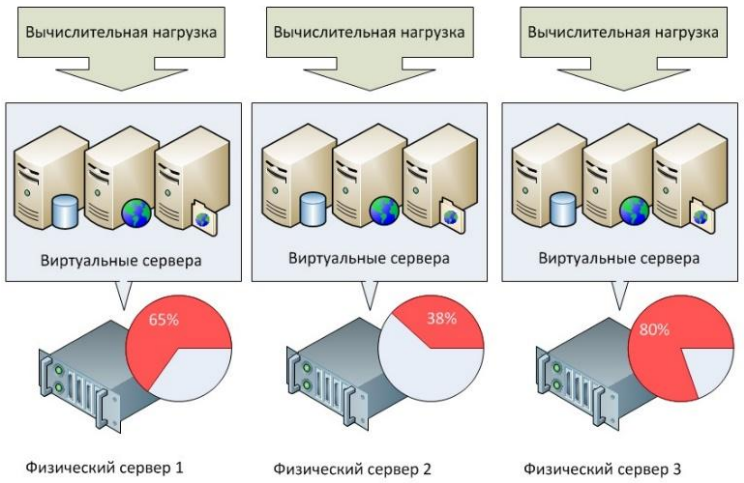


Рисунок 1 – Результаты мониторинга в гетерогенной среде

В результате мы выявили проблемы практики и проблемы теории.

Проблемы практики:

- Различные характеристики сетевого оборудования;
- Работа серверов в зависимости от технологии взаимодействия с клиентами и дисциплины обработки запросов;
- Не равномерная нагрузка между серверами и сетевым оборудованием.

Проблемы теории:

- Анализ работы серверов в зависимости от технологии взаимодействия с клиентами и дисциплины обработки запросов;
- Получение оптимальных параметров алгоритмов управления нагрузкой и выбор параметров серверов;
- Применяемый метод решения задачи управления нагрузкой;
- Существующие системы производят мониторинг системы, но не управляют распределением нагрузки.

После определения проблем практики и теории мы сформировали противоречие между необходимостью рационального распределение нагрузки на сетевое оборудование и отсутствие программного обеспечения для автоматизированного администрирования.

Мы поставили целью исследования: автоматизация информационных процессов загрузки системы, для автоматического управления сетевым оборудованием с управлением нагрузки виртуальных серверов.

Мы выявили границы – виртуальные сервера ОАО «Оренбургоблгаз».

Поиск программного обеспечения не дал положительных результатов, то есть не было найдено программных средств, которые могли бы в автоматическом режиме выполнять динамическое распределение нагрузки между сетевым оборудованием. В основном везде используется только мониторинг сети.

Возможно будет использован «мониторинг состояния вычислительных ресурсов в гетерогенной виртуальной среде» реализованный студентом – магистром Тыщенко С.В. или другое программное обеспечения, например, «Zabbix» или «10-Страйк: Мониторинг Сети» для слежения за состоянием сетевого оборудования.

Предположительно в компании ОАО «Оренбургоблгаз» используются горизонтальное (то есть на серверах приложений установлены компоненты приложений) или вертикальное (на серверах приложений установлены компоненты приложений, которые работают только с определенными базами данных) распределение нагрузки, как показано на рисунках 2 и 3.

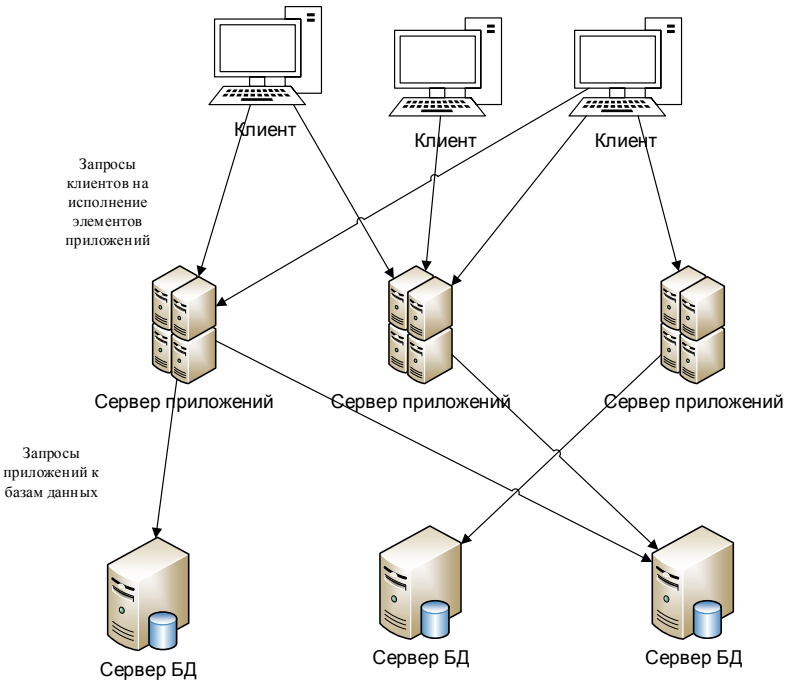


Рисунок 2 – Горизонтальное распределение приложений.

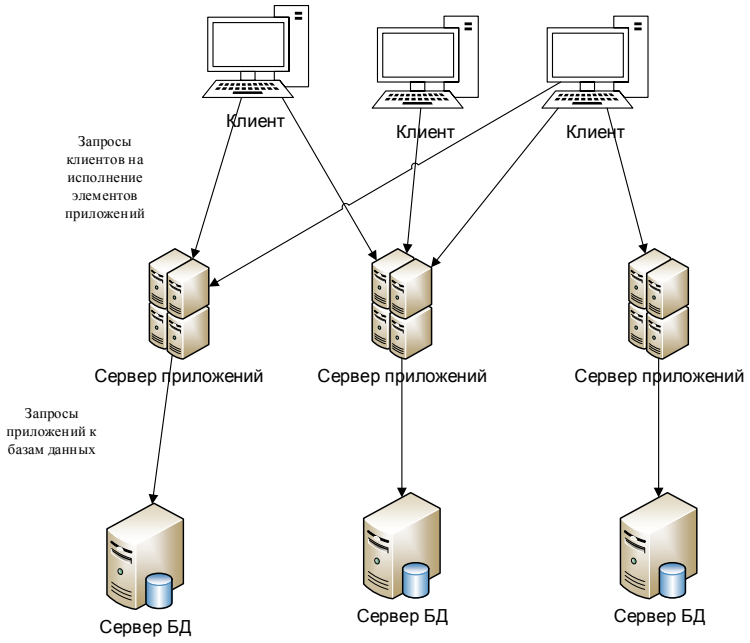


Рисунок 3 – Вертикальное распределение приложений.

Было решено реализовать метод «сервер – селектор» предложенный кандидатом технических наук Артемьевым А.Б., так как он является наиболее трудным в реализации и предполагает динамическое распределение нагрузки, что позволяет достичь максимальной производительности от сети. На рисунке 4 представлена предполагаемая структура сети.

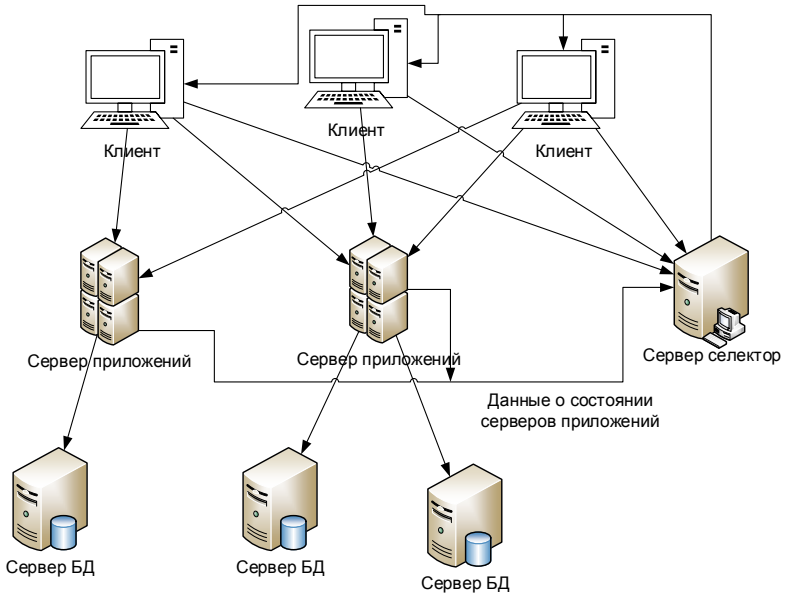


Рисунок 4 – Структура сети с использованием «сервер – селектор»

Селектор назначает сервер приложений клиенту, на основе анализа текущего состояния серверов приложений. Ниже представлены еще два вида возможной.

Для наглядного представления движения информационных потоков нами было использовано средство структурного моделирования Ramus educational, с использованием методологии диаграмм потоков данных DFD (Data Flow Diagram) и IDFE0 [3].

На рисунке 5 представлена контекстная диаграмма предметной области в нотации IDEF0.

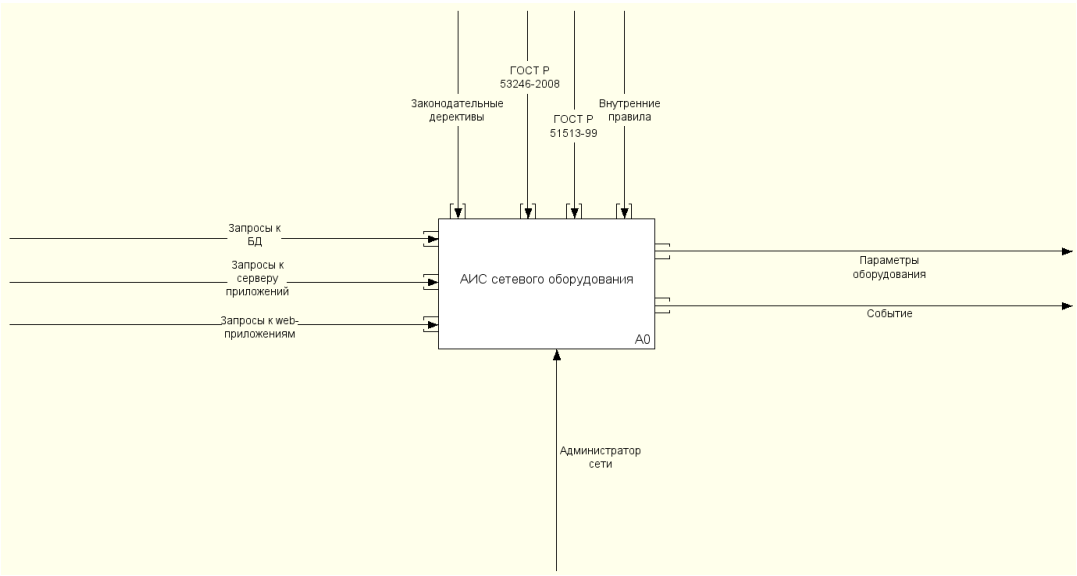


Рисунок 5 – Контекстная диаграмма в нотации IDEF0

Более детализированное функциональное описание, полученное путем декомпозиции общей диаграммы функционального описания, изображено на рисунке 6.

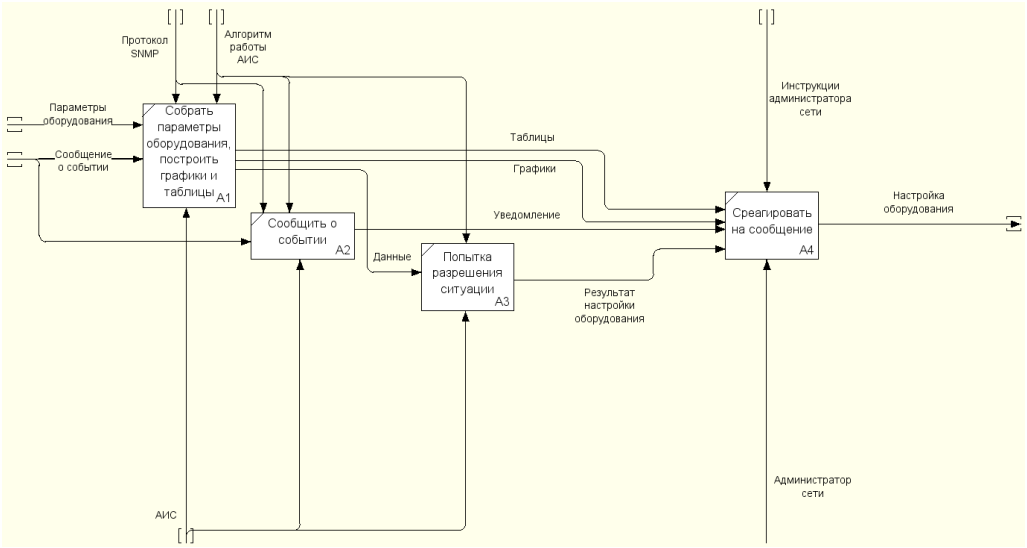


Рисунок 6 – Декомпозиция контекстной диаграммы

На рисунке 7 представлена диаграмма потоков данных АИС.

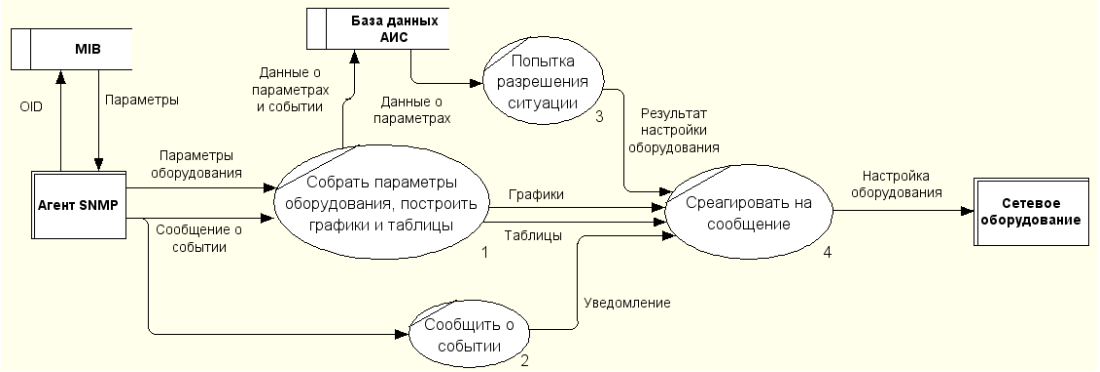


Рисунок 7 – Диаграмма потоков данных учреждения в нотации DFD

Сеть является главной линией получения и передачи информации, а сетевое оборудование – устройство, необходимое для её работы.

АИС отправляет запрос на получение необходимых данных агенту SNMP, который является частью программного обеспечения сетевого оборудования. Агент с помощью идентификатора параметра получает доступ к базе управляющей информации (MIB), которая хранит всю информацию о параметрах сетевого оборудования, и отправляет их АИС [4, 5].

АИС хранит полученную информацию на сервере в виде базы данных. На основе параметров, хранимых в базе данных, пытается разрешить проблему перегрузки сети. АИС уведомляет администратора сети о результате настройки с помощью интерфейса. Администратор сети, согласно инструкциям, выполняет настройку оборудования если это потребуется.

За основу магистерской диссертации будут взяты методы и алгоритмы, изложенные в диссертации на соискания технических наук Артемьева А.Б. «Разработка алгоритмов и моделей управления нагрузкой серверов в распределенных системах».

Список литературы

1. Компьютерные сети сегодня [Электронный ресурс]. – Режим доступа: https://sites.google.com/site/setevyetehnologiisgaki/setevye-tehnologii/istoria-koputernyh-setej/komputernye-seti-segodna – (Дата обращения: 14.10.2018).

2. Сетевое администрирование [Электронный ресурс]. – Режим доступа: http://inftis.narod.ru/adm/ais-n4.htm – (Дата обращения: 23.10.2018).

3. CASE-технология моделирования процессов с использованием средств BPWin и ERWin учебное пособие / А.Ф. Похилько, И.В. Горбачев. – Ульяновск: Ул ГТУ, 2008. – 120 с

4. SNMP: протокол управления сетью [Электронный ресурс] Режим доступа: http://www.laes.ru/list/pve/SNMP/tcp25.html. – (Дата обращения: 11.11.2018).

5. What is SNMP? Basic Tutorial on NMS, MIBs, OIDs, Traps & Agents [Электронный ресурс] Режим доступа: https://www.pcwdld.com/what-is-snmp-and-tutorial#nms. – (Дата обращения: 14.11.2018).

ВНУТРЕННИЕ ИДЕАЛЫ АЛГЕБР ЛИ И ИХ СВОЙСТВА

Мещерина Е.В., канд. физ.-мат.наук
Оренбургский государственный университет

Впервые понятие внутреннего идеала было введено для йордановых алгебр Н. Джекобсоном [1]. Первым систематическим изучением внутренних идеалов алгебр Ли занялась Дж. Бенкарт [2].

Определение. Скажем, что подпространство B алгебры Ли L является внутренним идеалом, если $[B,[B,L]]\subseteq B$.

Считается, что внутренний идеал алгебры Ли является аналогом одностороннего идеала ассоциативной алгебры.

Внутренние идеалы сыграли важную роль в классификации простых конечномерных алгебр Ли над полями положительной характеристики. В частности, было показано, что в любой конечномерной алгебре Ли над алгебраически замкнутым полем существуют одномерные внутренние идеалы [3] и [4].

Рассмотрим некоторые свойства внутренних идеалов алгебр Ли.

1. *Пусть алгебра Ли B является внутренним идеалом алгебры Ли L. Тогда B′ = [B,B] является внутренним идеалом*. [5]

Напомним определение присоединенного отображения для алгебры Ли.

Определение. Пусть $x,y\in L$. Тогда линейное отображение $ad:L\to L$, определенное по формуле $ad\ x(y)=[x,y]$, называется присоединенным к элементу x.

Доказательство. Из тождества Якоби следует, что присоединенное отображение алгебры Ли является дифференцированием. Такое дифференцирование алгебры Ли называется внутренним [6].

Пусть элементы $b_1,b_2\in B,l\in L$. Тогда

$$\begin{aligned}[[b_1,b_2],l]&=-ad\,l([b_1,b_2])=-[ad\,l(b_1),b_2]-[b_1,ad\,l(b_2)]=\\&=-[[l,b_1],b_2]-[[b_1,l],b_2]=[[b_1,l],b_2]-[[b_2,l],b_1]).\end{aligned}\qquad(1)$$

Из формулы (1) следует включение $[B,[B,L]]\subseteq[[B,L],B]$.

Следовательно, $[[B,B],[B,[B,L]]]\subseteq[[B,B],[[B,L],B]]$. Из того, что B является внутренним идеалом следует, что $[[B,L],B]\subseteq B$.

Отметим, что $[[B,B],B]\subseteq[B,B]$.

Получили включение $[[B,B],[[B,B],L]]\subseteq[[B,B],B]]\subseteq[B,B]$.

Мы доказали, что B' является внутренним идеалом алгебры Ли L.

2. *Внутренний идеал алгебры Ли не всегда является алгеброй Ли.*

Пример такого внутреннего идеала был построен в [5] и приведен ниже.

Рассмотрим алгебру матриц F_n , $n\geq 4$ порядка n над полем F.

Введем следующее известное обозначение для матричных единиц. Через e_{ij} обозначим матрицу, у которой на пересечении i-ой строки и j-го столбца стоит 1, а все остальные элементы равны нулю.

Матричные единицы перемножаются по следующему правилу:

$e_{ik}e_{ij} = \delta_{kl}e_{ij}$, где $\delta_{kl} = \begin{cases} 1, & k = l \\ 0, & k \neq l \end{cases}$ – символ Кронекера.

Рассмотрим алгебру A порожденную как векторное пространство всеми матричными единицами e_{ij}, $j > i$.

Алгебру A можно также охарактеризовать как алгебру верхнетреугольных матриц с нулями на главной диагонали.

Алгебра A является ассоциативной нильпотентной алгеброй. Она также является нильпотентной алгеброй Ли по отношению к операции коммутирования $[x,y] = xy - yx$.

Пусть B векторное подпространство, порожденное матричными единицами e_{12},e_{23}, а C – матричными единицами $\{e_{ij} \mid j - i \geq 3\}$.

Обозначим через D алгебру $D = B + C$.

Легко проверить, что $[D,[D,L]] \subseteq C$. Следовательно, D – внутренний идеал.

Коммутатор $[e_{12}, e_{23}] = e_{13}$ не содержится в D.

Следовательно, внутренний идеал D не является алгеброй Ли.

3. *Взаимный коммутант внутренних идеалов может не быть внутренним идеалом*. [5]

Рассмотрим пример. Он построен на основе примера из [2].

Рассмотрим алгебру Ли $sl_2(F)$ над полем F характеристики 0.

Тогда матрицы

$$e = e_{12},\ f = e_{21},\ h = e_{11} - e_{22}$$

образуют базис алгебры $sl_2(F)$ и подпространства Fe и Ff являются ее внутренними идеалами.

Рассмотрим множество $B = \{\alpha e \mid \alpha \in F\}$.

Покажем, что множество B является внутренним идеалом. Для этого нужно проверить, что $[B,[B,L]] \subseteq B$.

Вычислим коммутаторы базисных элементов:

$$[e, f] = [e_{12}, e_{21}] = e_{11} - e_{22} = h,$$
$$[e,h] = [e_{12}, e_{11} - e_{22}] = -e_{12} - e_{12} = -2e_{12} = -2e,$$
$$[f,h] = [e_{21}, e_{11} - e_{22}] = e_{21} + e_{21} = 2e_{21} = 2f,$$
$$[B,L] = span(e_{12}, e_{11} - e_{22}) = span(e,h).$$

Следовательно, $[B,[B,L]] \subseteq B$.

Возьмем множество $A = \{\beta f \mid \beta \in F\}$, которое так же является внутренним идеалом, и рассмотрим множество $C = [A, B] = \{\gamma h \mid \gamma \in F\}$.

Справедливы следующие соотношения

$$[h,e]=[e_{11}-e_{22},e_{12}]=2e_{12}=2e,$$
$$[h,f]=[e_{11}-e_{22},e_{21}]=-2e_{21}=-2f,$$
$$[C,L]=span(e_{12},e_{21})=(e,f),$$
$$[C,[C,L]]=span(e_{12},e_{21})=(e,f).$$

То есть, [*C*,[*C*,*L*]] не является подмножеством *C*, что означает, что множество *C* не является внутренним идеалом.

4. *Сумма внутренних идеалов алгебры Ли L может не быть внутренним идеалом*.

Например, в [5] была дана классификация внутренних идеалов алгебры $sl_2(F)$ над алгебраически замкнутым полем *F* характеристики нуль. Внутренними идеалами данной алгебры Ли являются подпространства $B_1=\{\alpha e_{12}|\alpha\in F\}$ и $B_2=\{\beta e_{21}|\beta\in F\}$ но их сумма $\alpha e_{12}+\beta e_{21}$ не является внутренним идеалом алгебры $sl_2(F)$.

5. *Если алгебра B является внутренним идеалом алгебры Ли L, то* $I=B\cap[B,L]$ *является идеалом B*. [5]

Доказательство. Пусть $x\in I$. Тогда $x\in B$ и $x\in[B,L]$.

Возьмем произвольный элемент $b\in B$ и рассмотрим [*b*, *x*]. Получим $[b,x]\in B$, $[b,x]\in[B,[B,L]]\Rightarrow[b,x]\in I$.

6. *Пусть подалгебра Ли B является внутренним идеалом алгебры Ли L. Тогда* B^n *– внутренний идеал*. [5]

Для доказательства напомним следующие определения.

Определение. Характеристическим идеалом алгебры Ли называется идеал замкнутый относительно внутренних дифференцирований.

Определение. Характеристический идеал [*L*,*L*], обозначаемый *D*(*L*) = *L*' называется производным идеалом или коммутантом алгебры Ли *L*.

Определение. Производным рядом алгебры Ли *L* называется убывающая последовательность $L^{(1)}\supset L^{(2)}\supset...\supset L^{(n)}\supset...$ характеристических идеалов, определяемых рекуррентно $L^{(1)}=L'$, $L^{(n+1)}=[L^{(n)},L^{(n)}]$.

Определение. Нижним центральным рядом алгебры Ли *L* называется убывающая последовательность $L^1\supset L^2\supset...\supset L^n\supset...$ характеристических идеалов, определяемых рекуррентно $L^1=L$, $L^{n+1}=[L^n,L]$.

Утверждение, аналогичное свойству 6, для множества B^n доказано в [2].

Доказательство. Отметим, что коммутант алгебры Ли также является алгеброй Ли.

Докажем методом математической индукции.

1. Основание индукции. Пусть *n* = 1.

Выше было доказано, что коммутант *B*' = [*B*,*B*] является внутренним идеалом (свойство 5).

2. Индукционный переход.

Предположим, что для $n = k$ утверждение выполнено, то есть $B^{(k)}$ является внутренним идеалом.

Докажем для $n = k + 1$.

По определению $B^{(k+1)} = [B^{(k)}, B^{(k)}]$.

Так как по предположению $B^{(k)}$ – внутренний идеал, то согласно свойству 1 делаем вывод, что $B^{(k+1)}$ является внутренним идеалом.

7. *Пусть H – внутренний идеал алгебры Ли L. Тогда справедливо включение* $[[H,H],L] \subset H$.[7]

Доказательство. Пусть $a,b \in H, x \in L$ – произвольные. Тогда справедливы равенства

$$[[a,b],x] = [[a,x],b] + [a,[b,x]] = -[b,[a,x]] + [a,[b,x]].$$

Из определения внутреннего идеала следует, что $[[a,b],x] \subset H$.

8. *В алгебре Ли $L = sl_n(F)$ над полем F характеристики нуль все собственные внутренние идеалы абелевы.*[7]

Доказательство. Пусть $H \subset sl_n(F)$ – неабелев собственный внутренний идеал.

Обозначим, через $A,B \in H$ матрицы такие, что $[A,B] \neq 0, X \in L$ – произвольная.

Тогда согласно свойству 7, справедливо включение $[[A,B],X] \in H$. Пусть $C = [A,B], C \neq 0$.

Рассмотрим два случая.

1. Матрица C является диагональной.

Так как $tr\ C = 0$, найдутся $1 \le i < j \le n$ такие, что коэффициенты при e_{ii}, e_{jj} равные α и β различные ненулевые.

Вычислим $[C, e_{ij}] = (\alpha - \beta)e_{ij}$. Из свойства 7 следует, что $e_{ij} \in H$.

Аналогично, получим включение $e_{ji} \in H$

i) Предположим сначала, что $C = \alpha e_{ii} + \beta e_{jj}$.

Применяя свойство 7, получим:

$$[C, e_{ik}] = \alpha e_{ik}, k \neq i, k \neq j \Rightarrow e_{ik} \in H,$$
$$[C, e_{kj}] = \beta e_{kj}, k \neq i, k \neq j \Rightarrow e_{kj} \in H,$$
$$[C, e_{ki}] = -\alpha e_{ki}, k \neq i, k \neq j \Rightarrow e_{ki} \in H,$$
$$[C, e_{jk}] = -\beta e_{jk}, k \neq i, k \neq j \Rightarrow e_{jk} \in H.$$

Согласно свойству 7, для $n = 2$ утверждение выполнено.

Теперь предположим, что $n \ge 3$.

Рассмотрим произведение $[[e_{ik}, e_{kj}], e_{ji}] = e_{ii} - e_{jj}$, где $k \neq i, k \neq j$.

Согласно свойству 7, справедливо включение $e_{ii} - e_{jj} \in H$.

Рассуждая аналогично, получим:

$$[[e_{ki}, e_{ii} - e_{jj}], e_{il}] = e_{kl}, \text{ где } k \neq i, k \neq j, l \neq i, l \neq j.$$

Следует, что $e_{kl} \in H$.

Вычислим

$$[[e_{kj}, e_{ji}], e_{ik}] = e_{kk} - e_{ii}, \text{ где } k \neq i, k \neq j.$$

Следует, что $e_{kk} - e_{ii} \in H$.

Аналогично

$$[[e_{ki}, e_{ij}], e_{jk}] = e_{kk} - e_{jj}, \text{ где } k \neq i, k \neq j.$$

Следует, что $e_{kk} - e_{jj} \in H$.

Пусть теперь $k \neq i, k \neq j, l \neq i, l \neq j$.

Получим $e_{kk} - e_{ll} = (e_{kk} - e_{jj}) + (e_{jj} - e_{ll})$.

Следует, что $e_{kk} - e_{ll} \in H$.

Мы доказали, что $H = L$.

ii) Предположим теперь, что в C входит с ненулевым коэффициентом слагаемое $\gamma e_{kk}, k \neq i, k \neq j$.

Тогда $\gamma \neq \alpha$ или $\gamma \neq \beta$.

Рассуждая аналогично предыдущему случаю, покажем, что $H = L$.

2. Матрица C не является диагональной.

Согласно свойству 7, для $n = 2$ утверждение выполнено.

Теперь предположим, что $n \geq 3$.

Пусть $t_1,...,t_n$ – базис векторного пространства V на котором матрица C задает линейное преобразование f.

Найдется $1 \leq i \leq n$ такое, что векторы t_i и $f(t_i)$ – неколлинеарны.

Пусть $s_1 = t_i$, $s_2 = f(s_1)$, векторы $s_3,...,s_n$ дополняют до базиса систему s_1, s_2.

Линейное преобразование f имеет матрицу

$$\begin{pmatrix} 0 & * & ... & * \\ 1 & * & ... & * \\ 0 & * & ... & * \\ ... & ... & ... & ... \\ 0 & * & ... & * \end{pmatrix}$$

в базисе $s_1,...,s_n$.

Обозначим через a_i вторую координату в разложении $f(s_i)$, $i \geq 3$ по базису $s_1,...,s_n$.

Введем новый базис $s_1' = s_1$, $s_2' = s_2$, $s_i' = s_i - a_i s_1$ при $i \geq 3$.

Тогда $f(s_i') = f(s_i - a_i s_1) = f(s_i) - a_i s_2$ при $i \geq 3$.

Тогда после перехода к базису $s_1',...,s_n'$ матрица C имеет вид

$$\begin{pmatrix} 0 & * & * & ... & * \\ 1 & \alpha & 0 & ... & 0 \\ 0 & * & * & ... & * \\ ... & ... & & ... & ... \\ 0 & * & & ... & * \end{pmatrix}$$

Согласно свойству 7, элемент $D = e_{11} - e_{22} + \alpha e_{12} = [C, -e_{12}]$ содержится в H.

Так же применяя свойство 7, получим элемент

$$F=[C,e_{13}]=\begin{pmatrix}0 & * & * & * & ... & * \\ 0 & 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 0 & 0 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & 0\end{pmatrix}$$

принадлежащий *H*.

Пусть

$$G=[D,-F]=\begin{pmatrix}0 & * & * & * & ... & * \\ 0 & 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 0 & 0 & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & 0\end{pmatrix}$$

Согласно свойству 7, элемент $e_{13}=[G,-e_{12}]$содержится в *H*.

Получим равенство $e_{13}=[e_{11}-e_{22}+\alpha e_{12},e_{13}]$.

Следовательно, $e_{13}\in[H,H]$.

Применяя свойство 7, получим элементы $e_{i3}, i\neq 3,$ и $e_{1j}, j\neq 1$.

Так как e_{12} принадлежит *H*, получим

$$e_{11}-e_{22}=(e_{11}-e_{22}+\alpha e_{12})-(\alpha e_{12}).$$

Следовательно, $e_{11}-e_{22}\in H$.

Вычислим $[e_{11}-e_{22},e_{12}]=2e_{12}$.

Следует, что $e_{12}\in[H,H]$.

Получим $[e_{31},e_{12}]=e_{32}$.

Следует, что $e_{32}\in H$.

Вычислим $[e_{32},e_{11}-e_{22}]=-2e_{32}$.

Следует, что $e_{32}\in[H,H]$.

Получим $[e_{23},e_{32}]=e_{22}-e_{33}$

Следует, что $e_{22}-e_{33}\in[H,H]$.

Из пункта 1 ii) получим равенство *H* = *L*.

9. *Пусть F – алгебраически замкнутое поле, char F = 0. Все собственные внутренние идеалы H алгебры Ли* $sl_n(F)$ *удовлетворяют условию:* $A,B\in H\Rightarrow AB=0$.[7]

Доказательство теоремы. Согласно теореме Ли [8], матрицы разрешимой алгебры Ли линейных преобразований конечномерного векторного пространства над алгебраически замкнутым полем характеристики нуль могут быть приведены одновременно к треугольному виду.

Согласно свойству 8 для полей нулевой характеристики все собственные внутренние идеалы *H* алгебры $sl_n(F)$ – абелевы.

Это означает, в частности, что H является абелевой алгеброй Ли.

Из теоремы Ли следует, что все матрицы собственного внутреннего идеала H могут быть приведены одновременно к треугольному виду.

Не трудно доказать, что диагональные элементы матриц из H равны нулю.

Пусть A и B две матрицы из H. Предположим, что матричные единицы $e_{kl}, k < l$ и $e_{ij}, i < j$ входят с ненулевыми коэффициентами в разложение A и B соответственно.

Тогда ненулевыми в коммутаторе $[A,B]$ могут быть только произведения $e_{kl}e_{ij}$, если $l = i$ (в этом случае $k < j$) или $e_{ij}e_{kl}$, если $j = k$ (в этом случае $i < l$).

Оба этих произведения не могут одновременно равняться нулю.

Следовательно, из равенства $[A,B] = 0$ следует равенство $AB = 0$.

10. Обобщим свойство 9 на один класс бесконечномерных алгебр Ли. [7]

Определение. Обозначим через $gl_{fr}(V)$ множество линейных отображений конечного ранга бесконечномерного векторного пространства V над полем F в себя. Пусть $sl_{fr}(V) = [gl_{fr}(V), gl_{fr}(V)]$.

Пусть F – алгебраически замкнутое поле, char $F = 0$, V – бесконечномерное векторное пространство над F. Все собственные внутренние идеалы H алгебры Ли $sl_{fr}(V)$ удовлетворяют условию: $f, g \in H \Rightarrow f \circ g = 0$.

Доказательство. Пусть H – собственный внутренний идеал алгебры Ли $sl_{fr}(V)$, $f, g \in H$ – произвольные.

Так как f,g – преобразования ограниченного ранга, существует векторное пространство $W \subset V$ такое, что $f(V), g(V) \subset W$.

Пусть $x \in V$ – произвольное.

Обозначим через U конечномерное подпространство V содержащее W и x.

Тогда ограничивая действие элементов H на U получим множество преобразований $G = H|_U$.

Покажем, что G – внутренний идеал алгебры Ли $sl(U)$.

Пусть $l \in sl(U), s,t \in H$. Обозначим через U' подпространство дополняющее U до V, то есть сумма $V = U \oplus U'$ – прямая.

Можно считать, что $l \in sl_{fr}(V)$, определяя действие l на U' нулевым образом.

Тогда $[s,[t,l]] \in H$.

Ограничивая действие преобразования $[s,[t,l]]$ на подпространстве U, получим $[s,[t,l]] \in G$.

Возможны 3 случая.

1. $G = 0$.

В этом случае $f \circ g(x) = 0$.

2. Подпространство G – собственный внутренний идеал алгебры Ли $sl(U)$.

Согласно свойству 9, выполнено равенство $f \circ g(x) = 0$.

3. $G = sl(U)$.

Обозначим через n размерность векторного пространства U.

Пусть $e_1, e_2, \ldots$ − базис векторного пространства V, первые n элементов которого образуют базис U.

Будем использовать обычные обозначения для матричных единиц.

Выполнено равенство $[sl(u), sl(u)] = sl(u)$.

Следующие коммутаторы принадлежат H:

$$[e_{ii} - e_{jj}, [e_{ii} - e_{jj}, e_{ik}]] = e_{ik}, [e_{ii} - e_{jj}, [e_{ii} - e_{jj}, e_{kj}]] = e_{kj}$$

где $i \neq j, i, j \leq n, k > n$.

Следовательно, $e_{ii} - e_{jj} \in [H, H], i, j > n,$ так как $e_{ii} - e_{jj} = [e_{ij}, e_{ji}]$.

Элементы $e_{ij} = \frac{1}{2}[e_{ii} - e_{jj}, e_{ij}]$ принадлежат H.

Мы показали, что все элементы вида $e_{ii} - e_{jj}, e_{ij}, i, j = 1,2,\ldots$ принадлежат H.

Пусть $h \in H$ − произвольное.

Учитывая ограниченность ранга f, можно считать, в бесконечной матрице A задающей f ненулевыми являются только первые k-1 строк.

Пусть A_i − матрица, состоящая из i-ой строки матрицы A. Тогда $A = A_1 + \ldots + A_{k-1}$.

Матрица $[e_{ik}, [e_{ki}, A_i]]$, $1 \leq i \leq k$-1 отличается от матрицы A_i конечным числом элементов.

Поэтому можно считать, что все A_i принадлежат H, $1 \leq i \leq k$-1.

Следовательно, $H = sl_{fr}(V)$.

В этом случае внутренний идеал H не является собственным.

Список литературы.

1. Jacobson, N. Structure theory of quadratic Jordan algebras / N. Jacobson // Lecture Notes.- Tata Institute.- Bombay, 1970.- 128 pp.

2. Benkart, G. On inner ideals and ad-nilpotent elements of Lie algebras / G. Benkart // Transaction of the American Mathematical Society.- 1977.- V. 232.- P. 61-81.

3. Премет, А. А. Алгебры Ли без сильного вырождения / А.А. Премет // Математический сборник, 1986. - Т. 129 (171). - № 1, - С. 140-153.

4. Премет, А. А. Внутренние идеалы в модулярных алгебрах Ли / А.А. Премет // Весці АН БССР. Сер. фіз.-мат. навук, 1986. - № 5. - С. 11-15.

5. Мещерина, Е.В. О некоторых свойствах внутренних идеалов алгебры Ли / Е.В. Мещерина, С.А. Пихтильков //Вестник ОГУ.- 2013.- № 9 (158).- С. 110-114.

6. Бурбаки, Н. Группы и алгебры Ли (главы I-III) / Н. Бурбаки. - М.: Мир, 1976.- 496 с.

7. Мещерина, Е.В. О собственных внутренних идеалах простых алгебр Ли / Е.В. Мещерина, С.А. Пихтильков, О.А. Пихтилькова //Ученые записки Орловского государственного университета.- 2012.- № 6.- Часть 2.- С. 156-162.

8. Джекобсон, Н. Алгебры Ли / Н. Джекобсон. - М.:Мир, 1964.- 355 с.

АЛГЕБРАИЧЕСКИЕ МЕТОДЫ КРИПТОАНАЛИЗА В УЧЕБНОМ КУРСЕ «ОСНОВЫ КРИПТОАНАЛИЗА»

Михляева А.В., Благовисная А.Н.
Оренбургский государственный университет

Одной из основных задач освоения дисциплины «Основы криптоанализа» является приобретение навыков решения задач криптоанализа [1]. В учебной литературе [2-6] рассмотрены методы корреляционного, линейного и дифференциального криптоанализа, а также учебные задания, способствующие приобретению навыков раскрытия шифров данными методами.

Помимо дифференциального, линейного и корреляционного методов криптоанализа, разрабатываются и активно исследуются алгебраические методы анализа, основанные на описании процесса защиты информации в виде систем булевых нелинейных уравнений и последующем их решении. В отличие от статистических методов линейного и дифференциального анализа, применение алгебраических методов позволяет вычислять секретную информацию при наличии меньшего числа известных данных. Также важным преимуществом алгебраических методов является вычислительная эффективность.

Методы алгебраического анализа применяются к современным симметричным шифрам и конструкциям, их составляющим. Среди первых публикаций, посвященных алгебраическим атакам на поточные шифры и структурные элементы поточных шифров, появились статьи британского криптографа Николя Куртуа [7-9]. В работах описаны атаки на поточные шифры с фильтрующими и комбинирующими генераторами. Показан взлом аппаратно реализуемых генераторов поточных шифров Toyocrypt и LILI-128. В этих же работах описан взлом E0 – поточного шифра протокола Bluetooth. Для решения систем булевых уравнений, возникающих в процессе атак, применялись методы линеаризации.

Исследование поточного алгоритма шифрования в сотовой связи A5 можно найти в работах [10-11]. В [10] показан процесс получения системы булевых уравнений для анализа. В статье [110] представлены результаты алгебраического криптоанализа алгоритма A5/2.

Алгебраический анализ поточных шифров семейства RC4 представлен в статье [12]. Отличительной особенностью шифра RC4 от рассмотренных ранее шифров является отсутствие линейных регистров сдвига в структуре шифра. В работе показана схема составления системы алгебраических уравнений, исследованы облегченные версии шифра RC4 и систем уравнений для них. Отмечено, что для шифра RC4 решить полученные системы известными методами не представляется возможным, то есть шифр RC4 считается стойким к алгебраическим атакам.

Изучение блочных шифров на стойкость к алгебраическим атакам также проводилось исследователями. В работах Николя Куртуа и его соавторов встречаются теоретические схемы описания алгебраических атак на блочные

шифры DES, AES и Serpent, а также на российский стандарт шифрования ГОСТ 28147-89. Несмотря на достаточно заметный интерес исследователей к алгебраическим атакам блочных шифров, на данный момент реализация алгебраических атак возможна лишь для упрощенных моделей существующих стандартов блочного шифрования при наличии ряда дополнительных условий, необходимых для анализа шифра.

Разнообразны и методы алгебраических атак на блочные шифры. Например, на упрощенные алгоритмы шифрования Rijndael алгебраические атаки проводились методами линеаризации и релинеаризации. Методами, использующими SAT-решатели и булевы базисы Грёбнера, предлагалось изучение стойкости к алгебраическим атакам алгоритма блочного шифрования SMS4, используемого в Китае в качестве национального стандарта для беспроводных локальных сетей. Также следует отметить появление описания атак на новый российский стандарт блочного шифрования ГОСТ Р 34.12-2015. Например, в статье [13] приведено описание алгебраического метода анализа стойкости шифров ГОСТ Р 34.12-2015 с размером блоков n=64 и n=128 бит методом релинеаризации.

Таким образом, уровень развития алгебраических методов криптоанализа шифров таков, что необходимо рассматривать вопросы алгебраического анализа криптосистем и криптографических примитивов в учебных дисциплинах. В некоторых учебных изданиях [5, 6], предназначенных для студентов вузов, встречаются разделы, посвященные криптографическим свойствам, которыми должны обладать булевы функции для обеспечения стойкости шифров к алгебраическим криптоатакам. В этих же книгах можно найти и формулировки заданий на раскрытие шифров методами алгебраического криптоанализа.

Рассмотрим примеры учебных задач, направленных на приобретение навыков решения задач криптоанализа алгебраическими методами раскрытия шифров.

Поясним суть криптографической атаки на конкретных примерах. Алгебраическая криптографическая атака использует алгебраические свойства шифра или криптографических конструкций, из которых шифр состоит.

Алгебраический анализ криптографических конструкций состоит из двух основных этапов: сведения исходной криптографической задачи (вскрытия ключа или зашифрованной информации, нахождение коллизии и т.д.) к задаче решения системы полиномиальных уравнений над конечным полем и решения полученной системы полиномиальных уравнений одним из возможных способов.

Продемонстрируем первый этап алгебраического криптоанализа на примере алгебраической криптоатаки на фильтрующие и комбинирующие генераторы.

Фильтрующие генераторы строятся на основе линейного регистра сдвига. На вход подаётся последовательность, являющаяся для криптосистемы ключом. На выходе из регистра сдвига последовательность поступает в фильтр, где усложняется булевой функцией (рисунок 1).

В качестве функции усложнения выступает булева функция следующего вида

$$f\ \ x_1,\ldots,x_n\ =\left(\bigoplus_{k=1}^{n}\bigoplus_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k}x_{i_1}\cdot\ldots\cdot x_{i_k}\right)\oplus a_0. \qquad (1)$$

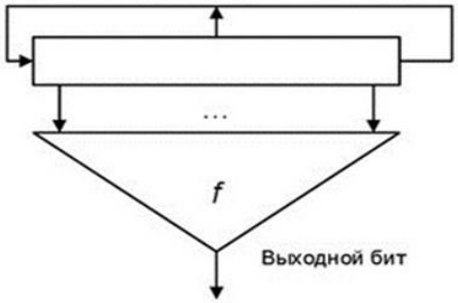


Рисунок 1 – Схема фильтрующего генератора

Рассмотрим криптографический генератор с регистром длины 3. В качестве функции усложнения выступает булева функция

$$f\ \ u_i,u_{i+1},u_{i+2}\ =u_iu_{i+1}u_{i+2}\oplus u_{i+1}u_{i+2}\oplus u_{i+1}\oplus u_{i+2}.$$

Пусть известен начальный отрезок гаммы: $\gamma=\ 1,1,0\ $.

Обозначим неизвестные переменные через u_0,u_1,u_2. Согласно данной схеме u_0,u_1,u_2 – начальное состояние регистра сдвига, которое является искомой ключевой последовательностью.

Система уравнений для поиска начального состояния генератора имеет вид:

$$\begin{cases} f\ \ u_0,u_1,u_2\ =u_0u_1u_2\oplus u_1u_2\oplus u_1\oplus u_2=1,\\ f\ \ u_1,u_2,u_3\ =u_1u_2\ \ u_0\oplus u_1\ \ \oplus u_2\ \ u_0\oplus u_1\ \ \oplus u_2\oplus u_0\oplus u_1=1,\\ f\ \ u_2,u_3,u_4\ =u_2\ \ u_0\oplus u_1\ \ \ u_1\oplus u_2\ \ \oplus\ \ u_0\oplus u_1\ \ \ u_1\oplus u_2\ \ \oplus u_0\oplus u_1\oplus u_1\oplus u_2=0. \end{cases} \qquad (2)$$

После преобразований уравнений системы, заключающихся в раскрытии скобок и приведении подобных слагаемых, получим систему

$$\begin{cases} u_0u_1u_2\oplus u_1u_2\oplus u_1\oplus u_2=1,\\ u_0u_1u_2\oplus u_0u_2\oplus u_0\oplus u_1\oplus u_2=1,\\ u_0u_1u_2\oplus u_0u_1\oplus u_1u_2\oplus u_0\oplus u_1\oplus u_2=0. \end{cases} \qquad (3)$$

Комбинирующие генераторы строятся на основе нескольких линейных регистров сдвига. На вход подаётся последовательность, являющаяся для криптосистемы ключом. На выходе из регистра сдвига последовательность усложняется булевой функцией (рисунок 2). В качестве функции усложнения выступает булева функция вида (1).

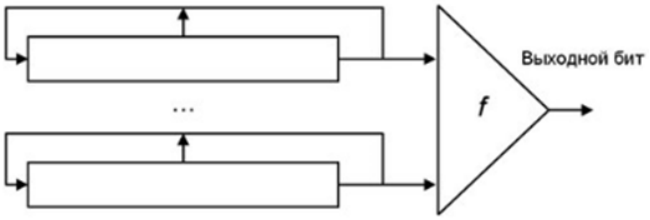


Рисунок 2 – Схема комбинирующего генератора

Рассмотрим криптографический генератор с двумя регистрами сдвига длины 2 и 3 соответственно. В качестве функции усложнения выступает булева функция $f(x_1, x_2) = x_1 x_2 \oplus x_2$. Пусть известен начальный отрезок гаммы: $\gamma = 0,1,0,0,1$. Обозначим неизвестные переменные через u_0, u_1, v_0, v_1, v_2. Согласно данной схеме, u_0, u_1, v_0, v_1, v_2 – начальное состояние регистра сдвига, которое является искомой ключевой последовательностью.

Система уравнений для поиска начального состояния генератора имеет вид:

$$\begin{cases} u_0 v_0 \oplus v_0 = 0, \\ u_1 v_1 \oplus v_1 = 1, \\ u_0 v_2 \oplus u_1 v_2 \oplus v_2 = 0, \\ u_0 v_0 \oplus u_0 v_1 \oplus v_0 \oplus v_1 = 0, \\ u_1 v_1 \oplus u_1 v_2 \oplus v_1 \oplus v_2 = 0. \end{cases}$$

Основным и самым сложным этапом алгебраического анализа шифра является решение систем нелинейных булевых уравнений.

В курсе «Основы криптоанализа» рассматриваются следующие методы решения систем булевых уравнений:

– поиск решения путём полного или частичного опробования возможных значений множества переменных;

– методы линеаризации;

– метод, основанный на поиске базисов Грёбнера.

Суть поиска решения путём полного или частичного опробования возможных значений множества переменных состоит в проверке возможных вариантов решений получающейся при алгебраической криптоатаке системы булевых уравнений.

Основная идея методов линеаризации заключается в том, чтобы путём преобразования системы свести её к линейной от большего числа переменных.

Продемонстрируем метод линеаризации для решения системы (3). Для упрощения системы нам понадобится понятие аннигилятора.

Булева функция g минимально возможной степени, не равная тождественно нулю, такая что $fg = 0$ или $f \oplus 1\ g = 0$, называется аннигилятором булевой функции f.

Для функций, имеющих небольшую алгебраическую степень и зависящую от небольшого числа переменных, поиск аннигиляторов можно осуществлять, используя определение аннигилятора. Аннигиляторы для функций $f = u_0u_1u_2 \oplus u_1u_2 \oplus u_1 \oplus u_2$ и $f \oplus 1 = u_0u_1u_2 \oplus u_1u_2 \oplus u_1 \oplus u_2 \oplus 1$ имеют вид: $g_1 = u_1u_2 \oplus u_1 \oplus u_2 \oplus 1$ и $g_2 = u_1 \oplus u_2$ соотвественно.

С помощью найденных аннигиляторов система (3) упростится до системы

$$\begin{cases} u_1u_2 \oplus u_1 \oplus u_2 \oplus 1 = 0, \\ u_2\ u_0 \oplus u_1\ \oplus u_2 \oplus\ u_0 \oplus u_1\ \oplus 1 = 0, \\ u_0 \oplus u_2 = 0. \end{cases} \quad (4)$$

Решение (4) имеет вид: $u_0 = 1,\ u_1 = 0,\ u_2 = 1.$

Методы решения систем нелинейных булевых уравнений, использующие базисы Грёбнера, являются обобщением метода Гаусса последовательных исключений переменных. Для системы уравнений базис Грёбнера – это набор многочленов, полученных в результате многошаговой редукции из исходных многочленов, которые задают систему.

Основные этапы решения системы на основе базисов Грёбнера:

– составление базиса Грёбнера на основе выбранного алгоритма его постоения (например, алгоритм Бухбергера) для идеала системы булевых уравнений;

– упрощение построенного базиса Грёбнера с помощью опреаций минимизации и редуцирования;

– составление и решение упростившейся системы.

Приведем результаты выполнения основных этапов решения системы (3). Первоначальный набор многочленов имеет вид:

$$f_1 = u_0u_1u_2 \oplus u_1u_2 \oplus u_1 \oplus u_2 \oplus 1, \quad f_2 = u_0u_1u_2 \oplus u_0u_2 \oplus u_0 \oplus u_1 \oplus u_2 \oplus 1, \quad f_3 = u_0u_1u_2 \oplus u_0u_1 \oplus u_1u_2 \oplus u_0 \oplus u_1 \oplus u_2. \quad (5)$$

В процессе поиска зацеплений и редукции к набору (5) добавляются ещё 6 многочленов:

$$f_4 = u_0u_2 \oplus u_1u_2 \oplus u_0,\ f_5 = u_0u_1 \oplus u_0 \oplus 1,\ f_6 = u_0 \oplus u_1 \oplus u_2,$$
$$f_7 = u_2 \oplus 1,\ f_8 = u_1u_2 \oplus u_1 \oplus u_2 \oplus 1,\ f_9 = u_1. \quad (6)$$

Совокупность многочленов (5) и (6) представляет собой базис Грёбнера. Упрощая, получаем следующий базис:

$$g_1 = u_0 \oplus u_1 \oplus u_2,\ g_2 = u_1,\ g_3 = u_2 \oplus 1. \quad (7)$$

Из данного набора составляем систему, решение которой имеет вид: $u_0 = 1, u_1 = 0, u_2 = 1$.

В заключение отметим, что представленные методы решения систем нелинейных булевых уравнений рассматривались на примерах с небольшим числом уравнений и неизвестных. С увеличением числа уравнений и неизвестных возникает потребность в программных средствах, осуществляющих решение систем, что приводит к необходимости поиска или реализации програмных средств для решения учебных задач дисциплины «Основы криптоанализа».

Список литературы

1. Рабочая программа дисциплины «Б.1.В.ДВ.6.2 Основы криптоанализа» / сост. А.Н. Благовисная. – Оренбург: ОГУ, 2018.

2. Бабенко, Л.К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. – Москва.: Гелиос АРВ, 2006. – 376 с.

3. Варлатая, С.К. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова. – Москва: Проспект, 2015. – 152 с.

4. Стандарт криптографической защиты – AES. Конечные поля / Под ред. М.А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.

5. Панкратова, И.А. Булевы функции в криптографии: учебное пособие / И. А. Панкратова. – Томск: Издательский Дом Томского государственного университета, 2014. – 88 с.

6. Токарева, Н. Н. Симметричная криптография. Краткий курс: учебное пособие / Н. Н. Токарева. – Н: Новосибирский государственный университет, 2012. – 232 с.

7. Courtois, N. Fast algebraic attacks on stream ciphers with linear feedback / N. Courtois // Lecture Notes in Computer Science. – Springer-Verlag, 2003. – vol. 2729. – P. 176-194.

8. Courtois, N. Higher Order Correlation Attacks, XL algorithm and Cryptanalysis of Toyocrypt [Электронный ресурс] / N. Courtois. – Springer, 2002. – Режим доступа: https://eprint.iacr.org/2002/087.pdf.

9. Courtois N., Algebraic Attacks on Stream Ciphers with Linear Feedback / N. Courtois, W. Meier // Eurocrypt 2003,Warsaw, Poland. – P. 345-359.

10. Vörös, M. Algebraic attack on stream ciphers [Электронный ресурс] / Martin Vörös // Master's Thesis. – Bratislava, 2007. – 68 p. – Режим доступа: http://www.dcs.fmph.uniba.sk/diplomovky/obhajene/getfile.php/master-mv.pdf?id=132&fid=219&type=application%2Fpdf.

11. Mihaita, A. Some Results on Algebraic Crypt Analysis of A5/2 Algorithm [Электронный ресурс] / A. Mihaita // Journal of Mobile, Embedded and Distributed Systems. – 2010. – vol. II, no. 1. – Режим доступа: https://www.scribd.com/document/76534878/Some-Results-on-Algebraic-Crypt-Analysis-of-A5-2-Algorithm.

12. Wong, K. KH. An Analysis of the RC4 Family of Stream Ciphers against Algebraic Attack [Электронный ресурс] / K. KH. Wong, G. Carter, E. Dawson // Proc. 8th Australasian Information Security Conference, Brisbane, Australia, 2010. – P. 67-74. – Режим доступа: http://crpit.com/confpapers/CRPITV105Wong.pdf.

13. Маро, Е. А. Реализация алгебраической атаки на шифры ГОСТ Р 34.12-2015 [Электронный ресурс] / Е.А. Маро // Инженерный вестник Дона, 2015. – № 4. – Режим доступа: http://www.ivdon.ru/uploads/article/pdf/IVD_176_Maro.pdf_81fed81a84.pdf.

ЧТО ТАКОЕ БЛОКЧЕЙН И ЧЕМ ЕГО ТЕХНОЛОГИЯ ОТЛИЧАЕТСЯ ОТ БАЗЫ ДАННЫХ

Мучкаева Е.А., Мурзаханова Э.И.
Оренбургский государственный университет

Привычные нам базы данных чаще всего используют архитектуру сети клиент-сервер. Пользователь (клиент) с разрешением, связанным с его учетной записью, может управлять данными, хранящимися на центральном сервере (добавлять, удалять, изменять их). Управление серверной частью остается за администраторами: они занимаются технической поддержкой, изменением структуры, если это требуется. Они также могут иметь различные уровни доступа, которые позволяют совершать различные действия.

Технология блокчейн отличается от традиционной базы данных архитектурой или самим принципом организации. В отличие от давно известных нам баз данных, внедрение blockchain предусматривает принцип отсутствия единого сервера и равноправного участия всех пользователей.

Но блокчейн также можно назвать базой данных, только отличия ее от классических баз кардинальны.

Блокчейн (BlockChain – цепочка блоков) представляет собой распределённую базу данных, где устройства хранения данных не имеют подключения к общему серверу. В данной базе данных хранится постоянно увеличивающийся список упорядоченных записей, называемых блоками. В каждом блоке содержится метка времени и ссылка на предыдущий блок.

При применении шифрования есть гарантия, что пользователями могут изменяться только те части цепочек блоков, которыми они могут «владеть» в случае, что они имеют закрытые ключи, без которых записи в файлы невозможны. Кроме того, при шифровании обеспечивается синхронизация копий распределённой цепочки блоков у других пользователей.

Представим «цифровой» студенческий дневник: каждая запись представляет собой такой блок. Эта запись имеет метку: дату и время. С самого начала предполагается обязательный запрет на внесение изменений записи задним числом, так как, записи о сдаче лабораторных, курсовых, зачетов, экзаменов и т.д. не должны допускать различных объяснений, а оставаться в исходном виде. К этим записям получают доступ только преподаватель, который владеет одним закрытым ключом, и студент, который владеет другим. Далее, к данной информации могут получить доступ только те, кому один из этих пользователей позволит воспользоваться своим закрытым ключом (например, университет в целом или отдельный факультет). Таким образом, можно использовать технологию блокчейн в базе данных университета.

Блокчейн – это универсальный инструмент для построения различных баз данных, который обладает следующими преимуществами:

1. Децентрализация. Отсутствует главный сервер хранения данных. Все записи хранятся у каждого участника системы.

2. Полная прозрачность. Любой участник может отследить все транзакции, проходившие в системе.

3. Конфиденциальность. Все данные хранятся в зашифрованном виде. Пользователь может отследить все транзакции, но не может идентифицировать получателя или отправителя информации, если он не знает номера кошелька. Для проведения операций требуется уникальный ключ доступа.

4. Надёжность. Любая попытка внесения несанкционированных изменений будет отклонена из-за несоответствия предыдущим копиям. Для легального изменения данных требуется специальный уникальный код, выданный и подтверждённый системой.

5. Компромисс. Данные, которые добавляются в систему, проверяются другими участниками. Если говорить умными словами – они пересчитывают хеш. (Хешированию посвящена отдельная статья, но по сути они считают яблоки с использованием сложных математических формул).

В данной технологии блокчейн первоначально заложен принцип безопасности на уровне базы данных. Она несомненно защищает данные, с которыми мы работаем, делая их при этом более доступными и прозрачными. Также, блокчейн заметно снижает затраты и минимизирует время, нужное при решении различных проблем и исправления ошибок.

В 2008 году Сатоши Накамото (Satoshi Nakamoto) выдвинул Идею цепочек блоков. А реализация ее осуществлена в 2009 году как компонент цифровой валюты — биткоина, при котором блокчейн играет роль главного общего реестра для всех операций.

В настоящее время мы уже часто делимся разными видами информации через децентрализованную интерактивную платформу интернета. А с технологией блокчейн предлагается заманчивая возможность избавления от данного «лишнего звена».

Технологию блокчейн можно использовать при хранении различных видов цифровой информации, включающего и компьютерный код. Данный фрагмент кода программируют так, чтобы его можно было выполнить, только если обе договаривающиеся стороны вводят свои ключи, то есть дают согласие на заключение контракта. Этот же код запрограммирован на получение информации из внешних потоков данных (метеорологические сводки, заголовки новостей и всё остальное, что может анализировать компьютер) и составление контрактов, которые могут быть автоматически зарегистрированы, если выполняются определённые условия.

Данный механизм называют «умные контракты» (смарт-контракты), и области их применения могут быть бесконечными.

С помощью данного подхода возможен контроль за использованием интеллектуальной собственности: он может определять, сколько раз пользователь имеет разрешение получения доступа к информации, поделиться этой информацией или скопировать её.

Пользуясь блокчейном каждый участник может поддерживать, вычислять и обновлять записи в базе данных. Все узлы работают вместе, все приходят к консенсусу, обеспечивая встроенную защиту сети.

С помощью блокчейна две стороны, «не доверяющие» друг другу, обмениваются информациями, без помощи посредника, центрального администратора. Транзакции обрабатывает сеть пользователей, которая выступает в роли механизма общего согласия. Таким образом децентрализованный контроль имеет большое значение, устраняя риски централизации.

В базе данных на блокчейне хранится информация, актуальная сейчас, а также вся информация, которая была раньше. С помощью данной технологии можно создавать базы данных, в которых есть история самих себя. Это дает возможность отследить любой момент времени.

Для сокрытия информаций на блокчейне требуется глубокая криптография и связанные с этим вычислительные нагрузки для узлов сети. Но это все-таки более эффективно, чем приватная база данных, построенная на классической основе.

Отсюда следует, что если конфиденциальность есть единственная цель, а доверие между сторонами установлено и нет проблемы с хранением больших объемов данных, базы на блокчейне не будет иметь для вас особых преимуществ.

Таким образом востребованность Блокчейна в настоящее время на высоком уровне, и 80% баз, используемых сейчас, есть необходимость в тех преимуществах, которые он имеет. Это и есть та основа, которая дает ему возможность такого быстрого распространения и получения большой поддержки. Внедрение блокчейна по определению сложный процесс, но основная идея технологии проста: распределенный реестр, запущенный одновременно на множестве (иногда можно говорить и о миллионах) узлов, распределенных по всему миру между различными пользователями и организациями. Уникальность блокчейна заключается в неизменности или необратимости, которую гарантирует криптографическая система защиты. Например, когда транзакции из реестра сгруппированы в блоки и записываются в базу данных, запись предваряет криптографическая верификация, в результате чего изменить состояние реестра путем каких-то уловок практически невозможно. В пользу доверия к блокчейну говорит и то, что любые изменения данных в цепочке блоков возможны, только если участники сети подтверждают законность транзакции в соответствии с общими правилами и протоколами.

Список литературы

1. Свон М. Блокчейн: Схема новой экономики. М.: Олимп-бизнес, 2017. - 240 с.

2. Соловьев А. Блокчейн: подводные камни // Открытые системы. СУБД. 2016. № 4. URL: http://www.osp.ru/os/2016/04/13050987/

О ЦЕЛЕСООБРАЗНОСТИ ИСПОЛЬЗОВАНИЯ ЛЕКЦИОННЫХ ЗАНЯТИЙ ПРОПЕДЕВТИЧЕСКОГО ХАРАКТЕРА ПРИ ИЗУЧЕНИИ МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН ГУМАНИТАРНЫХ НАПРАВЛЕНИЙ

Павленко А.Н., канд. физ. –мат. наук, доцент,
Пихтилькова О.А., канд. физ.-мат. наук, доцент
Оренбургский государственный университет

Как правило, изучение разделов математических дисциплин 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 для студентов гуманитарных направлений является сомнительной.

Следует отметить, что данной схемы изложения математического материала преподаватели часто придерживаются не только на математических и естественнонаучных, но и на гуманитарных направлениях. Очевидно, что данный способ изложения весьма абстрактного и часто громоздкого материала не способствует высокой мотивации к его изучению.

Рассмотрение в начале каждого раздела типичных задач, раскрывающих целесообразность введения нового математического понятия, как правило, полностью данную проблему не решает. 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, истории математики, естественнонаучных и гуманитарных дисциплин [2].

Вернувшись к введению понятия производной, можно отметить, что целесообразнее рассмотреть практически ориентированные задачи на максимум и минимум [3], некоторые задачи экономики и социологии, сводящиеся к дифференциальным уравнениям [4] и применение производной для получения приближенных формул [1], с помощью которых микрокалькулятор вычисляет, в частности, тригонометрические функции.

Для повышения эффективности учебного процесса при изучении математических дисциплин студентами гуманитарных направлений 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 [5].

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

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 в естествознании и гуманитарных дисциплинах.

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

На гуманитарных направлениях необходимо максимально использовать богатейшие возможности математики для формирования научного мировоззрения. Так, чтобы иметь представление об экспериментальном характере 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 [5]. 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.

При проведении пропедевтических занятий целесообразно максимально широко применять иллюстративные возможности информационных технологий. В частности, можно рассмотреть использование видеофайла при изучении алгоритма нахождения экстремума функций двух [1]. Данный видеофайл (рисунки 1-6) наглядно демонстрирует зависимость вида графика функции в окрестности стационарной точки при изменении величины Δ.

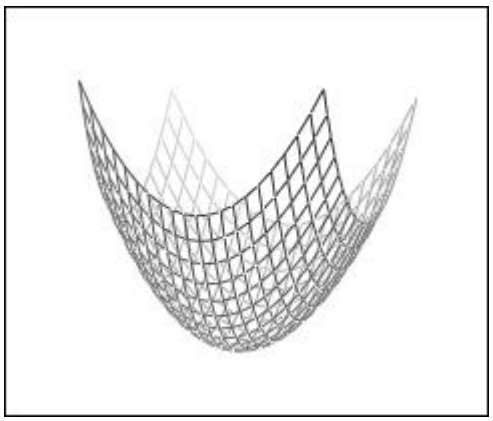


Рисунок 1

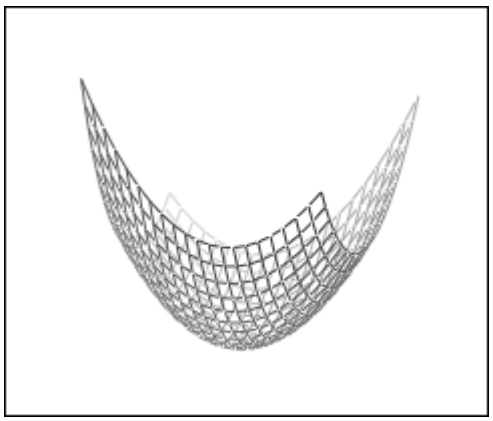


Рисунок 2

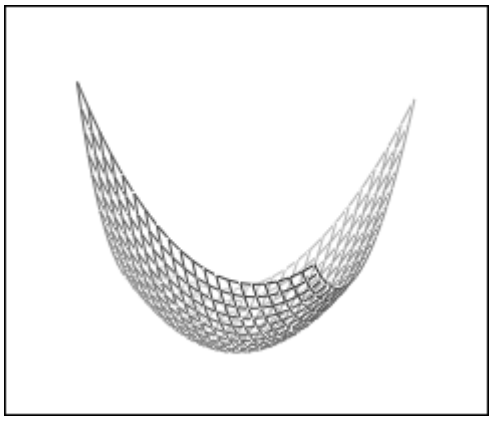


Рисунок 3

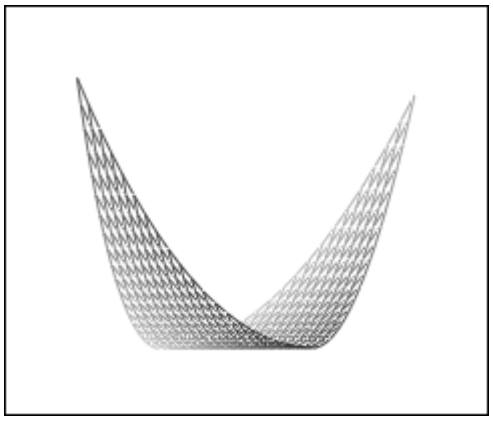


Рисунок 4

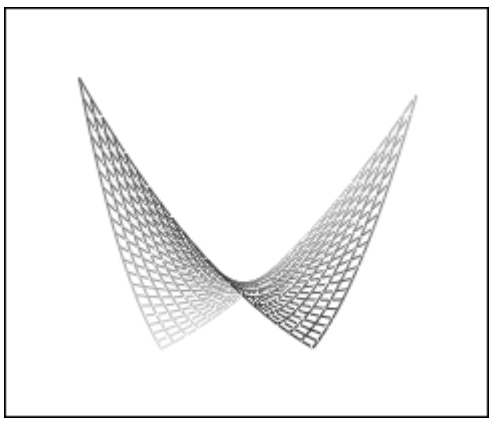


Рисунок 5

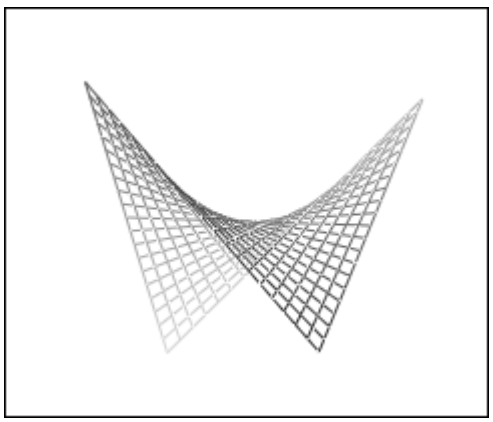


Рисунок 6

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. 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.

4. Битнер, Г.Г. Обыкновенные дифференциальные уравнения: учебное пособие / Г.Г. Битнер. – Ростов н/Д: Феникс, 2012. – 205 с. - ISBN 987-5-22219438-6.

5. Павленко, А.Н. О целесообразности использования лекционных занятий пропедевтического характера с применением мультимедийных технологий при изучении математических дисциплин естественнонаучных направлений [Электронный ресурс] / А.Н. Павленко, О.А. Пихтилькова // Университетский комплекс как региональный центр образования, науки и культуры: материалы Всерос. науч.-метод. конф. / Оренбург. гос. ун-т. – Электрон. дан. – Оренбург, 2017. – С. 2702-2706.

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.

ЗАДАЧА ОБОБЩЕННОЙ СОПРЯЖЕННОСТИ СЛОВ В КЛАССЕ ГРУПП С ОДНИМ ОПРЕДЕЛЯЮЩИМ СООТНОШЕНИЕМ

Пихтилькова О.А., канд. физ.-мат.наук, доцент,
Павленко А.Н, канд. физ.-мат.наук, доцент
Оренбургский государственный университет

В работе рассматривается класс групп, являющийся свободным произведением двух свободных групп с коммутирующими подгруппами: $G = \langle A * B; [H, K] = 1 \rangle$, где H, K - конечно порожденные подгруппы в A и B соответственно.

В статье будет дано решение проблема обобщенной сопряженности при условии, что подгруппы H и K удовлетворяют условию антинормальности.

Определение. Подгруппа P группы G называется антинормальной, если из того, что $g \notin P$ следует, что $g^{-1}Pg \cap P = 1$.

Определение. Под обобщенной проблемой сопряженности слов в группе G понимается решение в G системы уравнений $\&_{i=1}^{n} (z^{-1} w_i z = v_i), w_i, v_i, i = 1,..., n$ - фиксированные элементы группы G.

Существование такого алгоритма для некоторого класса конечно определенных групп позволяет для любого автоморфизма $\varphi \in AutG$ определить, является ли он внутренним.

Докажем следующую теорему.

Теорема. Существует алгоритм, позволяющий установить, пусто или нет пересечение следующих смежных подгрупп $\bigcap_{i=1}^{n} g_i C_g(w_i)$, где $C_g(w_i)$- централизатор элемента $w_i \in G$.

Доказательство. В [2] доказано, что централизатор любого элемента группы G, есть либо циклическая, либо абелева подгруппа с двумя образующими, либо одна из подгрупп вида

$$\left\langle s, \prod_{i=1}^{n} a_i K a_i^{-1} \right\rangle, a_i g a_i^{-1} \in H, g = s^k \notin H,$$

$$\left\langle s, K * \prod_{i=1}^{n} a_i K a_i^{-1} \right\rangle, a_i g a_i^{-1} \in H, g = s^k \in H,$$

$$\left\langle s, \prod_{i=1}^{n} b_i H b_i^{-1} \right\rangle, b_i g b_i^{-1} \in K, g = s^k \notin K,$$

$$\left\langle s, H * \prod_{i=1}^{n} b_i H b_i^{-1} \right\rangle, b_i g b_i^{-1} \in K, g = s^k \in K.$$

Доказательство теоремы будем вести последовательно, рассматривая пересечение $g_1 C_G(w_1) \cap g_2 C_G(w_2)$, где $g_1 C_G(w_1), g_2 C_G(w_2)$ - одна из подгрупп , указанных выше.

1. $C_G(w_1), C_G(w_2)$ – циклические подгруппы. Пусть $C_G(w_1) = \langle v_1 \rangle, v_1 = a(1)b(1)...a(\tau)b(\tau);\ C_G(w_2) = \langle v_2 \rangle, v_2 = a'(1)b'(1)...a'(\tau)b'(\tau).$

Если рассматриваемое пересечение не пусто, то для некоторых $g_1, g_2 \in G$ выполняются следующее равенство:

$$g_1(a(1)b(1)...a(\tau)b(\tau))^k = g_2(a'(1)b'(1)...a'(\gamma)b'(\gamma))^l. \quad (1)$$

Данное равенство рассматривается в группе G, так как решение данной проблемы в свободной группе $A * B$ тривиально. Выполнив в левой и правой частях свободные и R- сокращения, если такие есть, получим: $(g_2')^{-1} g_1'(a(1)b(1)...a(\tau)b(\tau))^{k'} = (a'(1)b'(1)...a'(\gamma)b'(\gamma))^{l'}$. Заметим, что из структуры диаграммы , соответствующей равенству

$$g_1'(a(1)b(1)...a(\tau)b(\tau))^{k'}(g_2'(a'(1)b'(1)...a'(\gamma)b'(\gamma))^{l'})^{-1} = 1$$

следует, что все b – слоги лежат в одном смежном классе по подгруппе K, соответствующие a –слоги равны и лежат в подгруппе H , а слоговые длины левой и правой частей совпадают. Поступим далее следующим образом: пусть отображение ψ ставит в соответствие каждому последнему b - слогу левой части(1) соответствующий b – слогу правой части: $\psi(b(t)) = k_1^1 b'(i_1) k_1^2$; $\psi(b(2t)) = k_2^1 b'(i_2) k_2^2$; $\psi(b(3t)) = k_3^1 b'(i_3) k_3^2$ и так далее.

Если при таком отображении для некоторых $r,s \in N$ $\psi(b(rt)) = k_r^1 b'(i_r) k_r^2$ и $\psi(b(st)) = k_s^1 b'(i_s) k_s^2$, то есть одному и тому же слогу в левой части равенства (1) соответствуют некоторые слоги левой части, отличающейся лишь k - слогами. Тогда, в силу антинормальности подгруппы K получаем, что $k_r^1 = k_s^1, k_r^2 = k_s^2$. Удалим часть слова между повторяющимися слогами, оставив один из них. Поступая таким же образом и далее, добьемся того, чтобы повторений не было. Но тогда показатель степени в левой части не превосходит числа γ. Зафиксировав показатель $k' \le \gamma$, составляем в подгруппе $C_G(w_2)$ множество слов $u_i, i \in N$ со слоговой длиной равной слоговой длине слова $(g_2')^{-1} g_1'(a(1)b(1)...a(\tau)b(\tau))^{k'}$.

Если для некоторого $k' \le \gamma$ равенство $(g_2')^{-1} g_1' = u_i(a(1)b(1)...a(\tau)b(\tau))^{-k'}$ выполняется, то пересечение смежных классов не пусто.

2. $C_G(w_1), C_G(w_2)$ – циклическая подгруппа и абелева с двумя образующими соответственно.

$C_G(w_1) = \langle v_1 \rangle, v_1 = a(1)b(1)...a(\tau)b(\tau); C_G(w_2) = \langle a, v_2 \rangle, v_2 = a'(1)b'(1)...a'(\gamma)b'(\gamma)$,причем элементы $a, a'(1)b'(1)...a'(\gamma)b'(\gamma)$ связаны следующей системой условий:

$$\begin{cases} (a'(1))^{-1} a a'(1) \in H \\ ... \\ (a'(\gamma-1))^{-1}...(a'(1))^{-1} a a'(1)...a'(\gamma-1) \in H \\ (a'(\gamma))^{-1}...(a'(1))^{-1} a a'(1)...a'(\gamma) \in H \\ b(1), b(2), ..., b(\gamma) \in K \end{cases}.$$

Предположим, что в группе G для некоторых g_1, g_2 выполнено равенство $g_1(a(1)b(1)...a(\tau)b(\tau))^k = g_2 a^x (a'(1)b'(1)...a'(\gamma)b'(\gamma))^l$.

Произведя в левой и правой частях равенства свободные и R-сокращения, получим $g_1^{'}(a(1)b(1)...a(\tau)b(\tau))^{k'} = g_2^{'}(a'(1)b'(1)...a'(\gamma)b'(\gamma))^{l'}a^x$.

Рассуждая как и в первом случае, приходим к тому, что значение k' не превосходи γ. Строим в подгруппе $C_G(w_2)$ для некоторого $k' \le \gamma$ множество слов $v_i, i \in N$ со слоговой длиной, равной $\left\| (g_2^{'})^{-1} g_1^{'}(a(1)b(1)...a(\tau)b(\tau))^{k'} \right\|$. Если после всех сокращений произведение $(g_2^{'})^{-1} g_1^{'}(a(1)b(1)...a(\tau)b(\tau))^{k'} u^{-1}$ принадлежит циклической подгруппе $\langle a \rangle$, то пересечение рассматриваемых смежных классов не пусто.

3. $C_G(w_1), C_G(w_2)$ - свободные абелевы группы ранга 2, образующие которых связаны соответствующими системами условий.

Из случаев 1, 2, 3 следует, что можно построить пересечение любой конечной последовательности смежных классов циклических подгрупп и абелевых с двумя образующими.

Случаи 4-6 рассматриваются аналогично и мы их не приводим.

Аналогичные рассуждения имеют место и при рассмотрении пересечения смежных классов централизаторов, среди которых есть подгруппы вида $\left\langle s, K * \prod_{i=1}^{n} a_i K a_i^{-1} \right\rangle, a_i g a_i^{-1} \in H, g = s^k \in H$. Теорема доказана.

Следствие. В группе G разрешима проблема пересечения конечного числа смежных классов подгрупп $C_G(w_i), i = 1...p$, где $w_i \in G$.

Теорема. В группе G алгоритмически разрешима проблема обобщенной сопряженности слов.

Доказательство. Пусть $v_i, i \in I$, $v_j, j \in I$ произвольные множества слов из группы G. Предположим, что существуют $z : z v_i z^{-1} = v_i$. Тогда

$$\begin{cases} z w_1 z^{-1} = v_1 \\ z w_2 z^{-1} = v_2 \\ ... \\ z w_n z^{-1} = v_n \end{cases} . \quad (2)$$

Так как для данного класса групп разрешима проблема сопряженности, то существуют такие $z_1, z_2, ..., z_n \in G$, что

$$\begin{cases} z_1 w_1 z_1^{-1} = v_1 \\ z_2 w_2 z_2^{-1} = v_2 \\ ... \\ z_n w_n z_n^{-1} = v_n \end{cases} . \quad (3)$$

Из (2) и (3) :

$$\begin{cases} z_1 w_1 z_1^{-1} = z w_1 z^{-1} \\ z_2 w_2 z_2^{-1} = z\ w_2 z^{-1} \\ \dots \\ z_n w_n z_n^{-1} = z\ w_n z^{-1} \end{cases}, \qquad \begin{cases} z_1^{-1} z w_1 z^{-1} z_1 = w_1 \\ z_2^{-1} z w_2 z^{-1} z_2 = w_2 \\ \dots \\ z_n^{-1} z w_n z^{-1} z_n = w_n \end{cases}.$$

.

Из последней системы видно, что $z_1^{-1} z \in C_G(w_i), i = 1...n.$ Положим $z_1^{-1} z = n_i, i = 1...n$. Тогда

$$\begin{cases} z_1^{-1} z = n_1 \\ z_2^{-1} z = n_2 \\ \dots \\ z_n^{-1} z = n_n \end{cases}, \qquad \begin{cases} z = z_1 n_1 \\ z = z_2 n_2 \\ \dots \\ z = z_n n_n \end{cases}, \qquad \begin{cases} z = z_1 n_1 \\ \begin{cases} z_1 n_1 = z_2 n_2 \\ \dots \\ z_1 n_1 = z_n n_n \end{cases} \end{cases}.$$

Следовательно, задача нахождения z сводится к решению проблемы пересечения смежных классов централизаторов, которая решена для данного класса групп. Теорема доказана.

Далее, как следствие получаем теорему.

Теорема. Пусть $G = \langle A * B; R, K = 1 \rangle$ конечно определенная группа и $\forall w_i\ _{i=1..n}$, $\forall v_i\ _{i=1..n}$ слова из группы G. Если F - какое-то решение системы $\&_{i=1}^{n} (z^{-1} w_i z = v_i), w_i, v_i, i = 1,..., n,$ то множество $C_G(H) * F$, где $C_G(H)$ – централизатор подгруппы H, порожденный множеством $\forall w_i\ _{i=1..n}$, является множеством всех решений системы.

Список литературы

1 Кавуцкий М. А., Молдаванский Д. И. Об одном классе групп с одним определяющим соотношением // Алгебраические и дискретные системы. Межвузовский сборник научных трудов. Иваново. 1988. С. 35-48.

2 Новикова О.А. Решение алгоритмических проблем для свободного произведения с коммутирующими подгруппами: дис. … канд. ф.-м. н. Моск. пед. университет, Москва, 2002.

3 Линдон Р., Шупп П. Комбинаторная теория групп. М.: Мир, 1980.

4 Логинова Е. Д. Финитная аппроксимируемость свободного произведения двух групп с коммутирующими подгруппами // Сиб. мат. ж. 1999. Т. 40, N 2. С. 395-407.

5 Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. М.: Наука, 1974.

6 Масси У.. Столлингс Дж. Алгебраическая топология. Введение. М.: Мир, 1977.

7 Нещадим М. В. Свободные произведения групп не имеют внешних нормальных автоморфизмов // Алгебра и логика. 1996. 5. С. 562-566.

8 Brunner A. On a class of one-relator groups // Can. J. Math. 1980. V. 32. N 2. P. 414-420.

9 Wise D. T. A continually descending endomorphism of a finitely generated residually finite group // Bull. Lond. Math. Soc. 1999. V. 31. P. 45-49

10 Тьеджо Д. О нормальных автоморфизмах некоторых групп с одним определяющим соотношением // Тезисы докладов международной научной конференции студентов, аспирантов и молодых ученых "Молодая наука-XXI веку", Иваново, 19-20 апреля 2001 г. С. 69.

ОБ ОДНОМ АЛГОРИТМЕ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ЭНДОМОРФНОЙ СВОДИМОСТИ

Пихтилькова О.А., канд. физ.-мат.наук, доцент,
Кравцова А.В.
Оренбургский государственный университет

В работе рассматривается криптография, основанная на группах («group-based cryptography»), - одно из современных направлений, главными объектами в котором являются абстрактные бесконечные группы, а основной целью - построение на их основе криптографических примитивов, протоколов и систем.

Основные исследования по этому направлению ведутся методами комбинаторной теории групп, сложности и теории вычислений. Обращается внимание на использование неразрешимых и трудноразрешимых алгоритмических поблем теории групп в качестве основы обозначенного построения.

Рассматриваются аспекты сложности алгоритмических проблем и связанные с ними проблем поиска. Поясняется универсальность диофантова языка в криптографии. Отмечается его объединяющая роль. В качестве одного их вариантов возможных платформ для криптографических примитивов и протоколов предлагается использовать свободные метабелевы группы.

Приводятся убедительные аргумены для такого использования, в том числе алгоритмическая разрешимость в этих группах проблемы равенства и наличие нормальных форм записи элементов группы. Ещё одним аргументом является алгоритмическая неразрешимость в таких группах проблемы существования решений у групповых уравнений и алгоритмическая неразрешимость проблемы эндоморфной сводимости, вытекающих из неразрешимости 10-й Проблемы Гильберта. Предполагается построение на свободных метабелевых группах возможно односторонних функций и протоколов аутентификации с нулевым разглашением.

Объект исследования – бесконечные группы.

Предмет исследования – методы теории групп, теории сложности и теории вычислений.

Цель работы – исследование бесконечных групп и построение на их основе возможно односторонних функций.

Пусть G - эффективно заданная группа, в которой разрешима проблема равенства и неразрешима проблема эндоморфной сводимости. Допустим, что нам необходимо построить на группе G одностороннюю функцию со значением также в G. Как правило, эффективно заданные группы конечно порождены. Поэтому предполагаем, что в G существует конечное порождающее множество $X_n = \{x_1,...,x_n\}$. Произвольный элемент g группы G записывается как групповое слово $g = g(x_1,...,x_n)$ от фиксированных порождающих элементов. Каждый эндоморфизм $\varphi : G \to G$ однозначно определяется своими значениями на

элементах порождающего множества X_n. Если $\varphi(x_i) = h_i$ для $i = 1,...,n$, то значением элемента $g = g(x_1,...,x_n)$ будет элемент $\varphi(g) = g(h_1,...,h_n)$. Однако не любое отображение $\varphi: X_n \to G$ продолжается до эндоморфизма в общем случае. Поэтому представляется перспективным выбирать в качестве группы G свободную группу конечного ранга некоторого многообразия групп L. Тогда любое отображение $\varphi: X_n \to G$, где X_n - базис группы G (т. е. множество свободных порождающих группы G в многообразии L), однозначно определяет эндоморфизм $\varphi: G \to G$. Для его задания достаточно определить образы базисных элементов, записав их в виде групповых слов от этих элементов. Ещё лучше, если в группе G есть нормальная форма записи элементов. Тогда эндоморфизм можно задать, записывая образы базисных элементов в этой нормальной форме. В работе [3] отмечено, что свободные метабелевы группы отвечают описанным требованиям.

Определим функцию $\varphi: G \to G$, сопоставляющую элементам группы, записанным в нормальной форме, нормальные формы их значений относительно эндоморфизма φ. Для эффективности соответствующих вычислений необходимо, чтобы в группе G существовал эффективный алгоритм записи элемента в нормальной форме по его представлению в виде группового слова от порождающих элементов или в каком-то другом виде, отвечающем эффективности задания группы G. Необходима также эффективная процедура вычисления нормальных форм обратного элемента и произведения элементов. Если группа G удовлетворяет этим требованиям, то получаем эффективно вычислимую функцию, определённую на множестве нормальных форм элементов группы G со значениями в этом же множестве. Если определить для элементов группы G некоторую функцию длины, например ввести на ней словарную метрику, то не существует полиномиального алгоритма, ограничивающего длину прообраза по длине образа для данной функции. Более того, никакая рекурсивная функция не даст такого ограничения. Не существует и других эффективных процедур, сводящих решение задачи поиска аргумента по значению функции к ограниченному полному перебору.

При этом, однако, возникает существенный вопрос об обращении функции на генерическом множестве значений. Возможно ли найти генерическое подмножество в множестве всех значений функции относительно естественной меры на этом множестве, на котором проблема поиска решается эффективно? Этот вопрос требует специального исследования в каждом конкретном случае (обзор [3] или более детальное изложение в [1, 2, 7]).

Отсюда можно вывести следующее общее заключение. Если бы длины значений $\varphi(x_i) = h_i$ для $i = 1,...,n$, соответствующие эндоморфизму ϕ, переводящему g в $f = f(c)$, можно было оценить сверху полиномиальными функциями от с, то проблема эндоморфной сводимости g к f в группе M была бы разрешимой. Поскольку это не так, подобной оценки не существует. Это приводит к невозможности переборного решения проблемы.

Относительно возможной эффективной обратимости рассматриваемой функции на генерическом множестве значений заметим, что в работе А. Н. Рыбалова [8] доказано, что 10-я Проблема Гильберта остается алгоритмически неразрешимой на любом строго генерическом множестве диофантовых уравнений.

Впервые идея использования рассматриваемой схемы для построения протокола аутентификации на платформе группы с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости была высказана В. А. Романьковым в докладе на семинаре в Graduate Center City University of New York в 2007 г. Впоследствии идея была описана в работе Д. Григорьева и В. Шпильрайна [9]. Авторы опирались на результаты В. А. Романькова из [3, 4].

В общих чертах протокол выглядит следующим образом.

У с т а н о в к а. Выбирается бесконечная эффективно заданная группа G с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости. Абонент **A** фиксирует публичный элемент g и f и секретный эндоморфизм φ, вычисляет и публикует образ $f = \varphi(g)$. Элементы g выбираются таким образом, чтобы проблема эндоморфной сводимости для пары (g, f) была трудна. Это означает, что по f трудно вычислить эндоморфизм φ, переводящий g в f.

Алгоритм аутентификации:

1) В качестве сессионного ключа выбирается эндоморфизм (в работе [9] автоморфизм) ψ, вычисляется элемент $v = \psi(f)$ и передается в систему C, в которой осуществляется аутентификация пользователя A.

2) Система C с равной вероятностью выбирает случайный бит и отсылает его A.

3) Если A получает 0, то он просто публикует ψ, а C проверяет, что действительно v - образ f относительно ψ. Если A получает 1, то он вычисляет композицию $\chi = \varphi\psi$, передает её C, который проверяет справедливость равенства $v = \chi(g)$.

Схема выглядит как протокол аутентификации с нулевым разглашением, аналогичный известному протоколу Фиата - Шамира (см., например, [25, 26]). Однако для её криптостойкости необходимо выполнение ряда дополнительных условий. Во- первых, необходимо, чтобы существовал фигурирующий в протоколе элемент g, проблема вхождения в множество эндоморфных образов которого алгоритмически неразрешима. Как объяснялось выше, это возможно, если в качестве группы G выбрать свободную метабелеву группу M_n достаточно большого ранга n. В этом случае элемент f можно брать случайным образом из фиксированного смежного класса по циклической подгруппе гр(h), полагая $f = f(c)$. Но далее аналогичные условия должны быть выполнены для пары элементов f, v. Результаты работы [4] уже не позволяют считать, что проблема вхождения в множество эндоморфных образов элемента f алгоритмически

неразрешима. Но даже если бы это было так, приведённых условий все равно оказалось бы недостаточно.

Для разрешения этой ситуации можно ввести определение группы с неразрешимой двукратной проблемой эндоморфной сводимости, а именно можно доказать, что в свободной метабелевой группе M_n достаточно большого ранга можно выбрать элемент g, элемент b, циклическую подгруппу гр(h), элемент u и конечно порождённую абелеву группу A таким образом, что для любой пары элементов (g, f), где $f \in b$ гр(h), и любой пары элементов (f, v), где $v \in uA$, одновременно алгоритмически неразрешимы проблемы эндоморфной сводимости. Более того, знание эндоморфизма χ, такого, что $\psi(f) = v$, не позволяет эффективно находить ни эндоморфизм φ, такой, что $\varphi(g) = f$, ни эндоморфизм ψ, такой, что $\psi(f) = v$. Наоборот, знание эндоморфизма ψ, такого что $\psi(f) = v$, не позволяет восстановить ни φ, ни χ. Легко видеть, что эти условия являются необходимыми в обеспечении криптостойкости приведённого алгоритма.

Соответствующие построения проводятся эффективно. Они также основываются на неразрешимости 10-й Проблемы Гильберта и интерпретации диофантовых уравнений в свободных метабелевых группах.

Приведенные далее скриншоты демонстрируют работу алгоритма аутентификации (рис. 1-3).

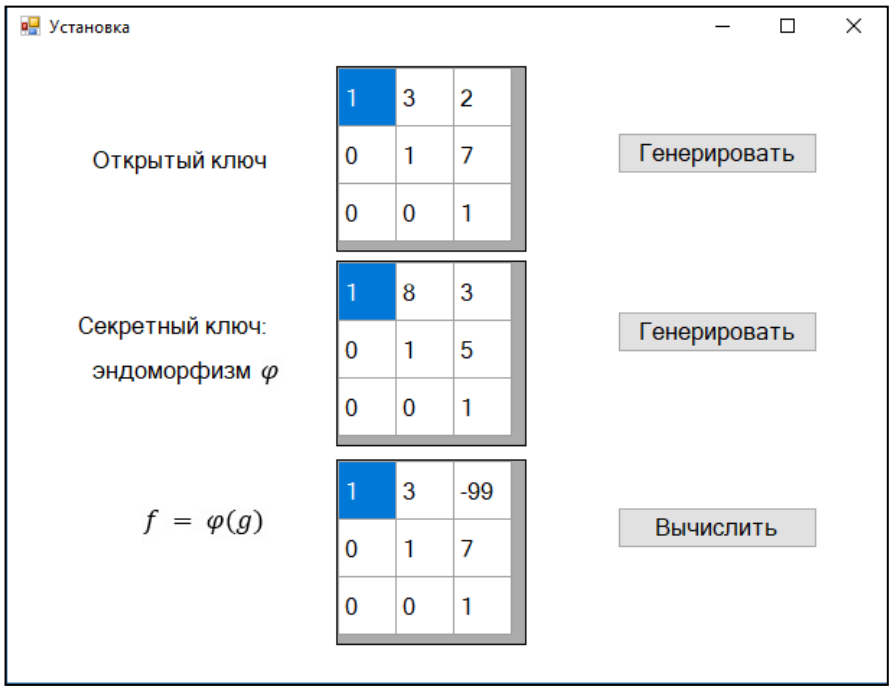


Рис. 1

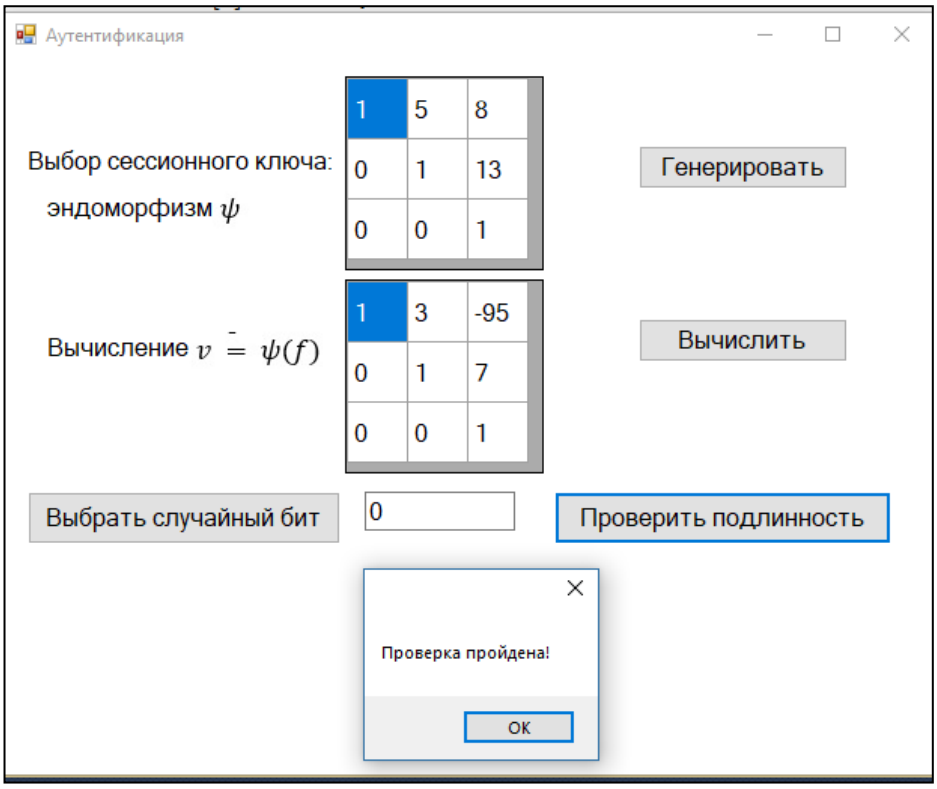


Рис. 2

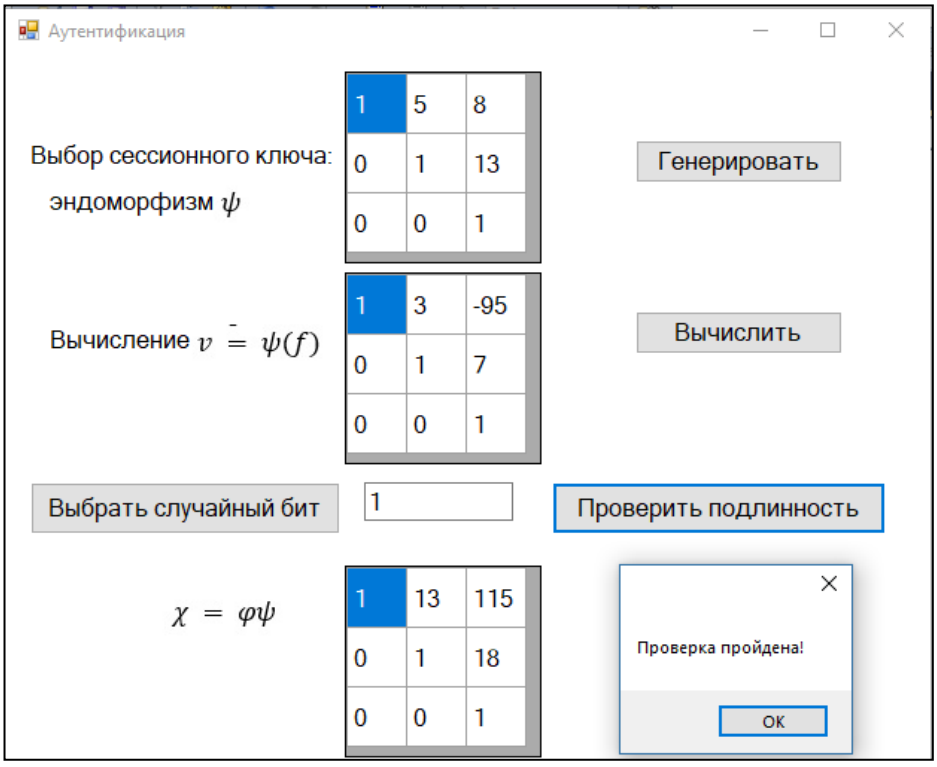


Рис. 3

Заметим также, что близкой по теме проблеме построения двукратной возможно односторонней функции посвящена работа [10]. Отсюда видно, что создание криптографических приложений, основанных на проблемах теории групп, имеет обратное влияние на развитие самой теории групп. Постановка

алгоритмических проблем приобретает новые формы. Отметим в этой связи возросший интерес к проблемам поиска. Вопросы теории сложности становятся все более актуальными и также приобретают новые формы. Достаточно ещё раз упомянуть понятие генерической сложности проблемы, возникшее главным образом при исследовании практических алгоритмов.

Список литературы

1 Myasnikov A., Shpilrain V., and Ushakov A. Group-based cryptography. (Advances courses in Math., CRM, Barselona). Basel, Berlin, New York: Birkh¨auser Verlag, 2008. 183 p.

2 Myasnikov A., Shpilrain V., and Ushakov A. Non-commutative cryptography and complexity of group-theoretic problems. (Amer. Math. Soc. Surveys and Monographs). Providence, RI: Amer. Math. Soc., 2011. 385 p.

3 www.grouptheory.info/PersonalPages/ Shpilrain, Vladimir/Cryptologye PrintArchive

4 Нейман Х. Многообразия групп. М.: Мир, 1974. 264 с.

5 Ремесленников В. Н., Романьков В. А. Теоретико-модельные и алгоритмические вопросы теории групп // Итоги науки и техн. Алгебра. Геометрия. Топология. Т. 21. М.: ВИНИТИ, 1983. С. 3–79.

6 Адян С. И., Дурнев В. Г. Алгоритмические проблемы для групп и полугрупп // Успехи матем. наук. 2000. Т. 55. С. 3–94.

7 Petrides G. Cryptoanalisis of the public key cryptosystem based on the word problem on the Grigorchuk groups // LNCS. 2003. V. 2898. P. 234–244.

8 Magyarik M. R. and Wagner N. P. A public key cryptosystem based on the word problem // LNCS. 1985. V. 196. P. 19–36.

9 Fine B., Habeeb M., Kahrobaei D., and Rosenberger G. Survey and open problems in noncommutative cryptography // JP J. Algebra, Number Theory and Applications. 2011. V. 21. P. 1–40.

10 Papadimitriou C. Computation complexity. Boston: Addison-Wesley, 1994. 523 p.

МОДЕЛИРОВАНИЕ ПРИЛОЖЕНИЙ ДЛЯ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Полежаев П.Н., Бахарева Н.Ф., д-р техн. наук, профессор,
Шухман А.Е., канд. пед. наук, доцент,
Ушаков Ю.А., канд. техн. наук, доцент, Легашев Л.В.
Оренбургский государственный университет

В настоящее время большие данные (big data) [1] находят применение в различных сферах деятельности человека, включая анализ сетевого трафика, журналов работы компонентов компьютерных инфраструктур, транзакций в банковской сфере (поиск мошеннических операций), а также в медицинской (ДНК, снимки томографии пациентов), экономической и картографической информации. Все больше крупных и средних компаний разрабатывают приложения для обработки больших данных, позволяющих повысить эффективность бизнес-процессов и получить дополнительную прибыль. Для обработки больших данных нередко применяют технологии облачных вычислений (cloud computing), в частности, возможно использование услуг одного или нескольких провайдеров публичных облачных услуг IaaS (Infrastructure as a Service). Виртуальные машины и сети могут быть использованы для развертывания отказоустойчивой масштабируемой инфраструктуры по обработке больших данных с гибкой системой оплаты (pay-as-you-go).

Каждое приложение (задача) для обработки больших данных, отправляемое в вычислительный сервис (Computations as a Service), может быть формализовано в виде следующего вектора:

$$App = (Jobs, DataStorages, User, T_{\max}),$$

где $Jobs = \{Job_i\}$ – множество заданий приложения, которые выполняются последовательно, например, последовательные запросы к источникам данных или несколько последовательных Map-Reduce преобразований; $DataStorages = \{DataStorage_i\}$ – конкретные источники входных данных и хранилища для сохранения результатов вычислений (файлы из распределенной файловой системы, например, HDFS – Hadoop Distributed File System [2]), данные из хранилища BLOBS (Binary Large Objects), из реляционной или NoSQL базы данных); $User \in Users$ – пользователь-владелец задачи, $T_{\max} \in N$ – максимальное время исполнения, заданное пользователем задачи.

Каждое задание Job_i представляет собой ориентированный ацикличный граф вычислительных стадий, который может быть формализован следующим образом:

$$Job_i = (Stages_i \cup DataStorages'_i, Precedence_i, Volume_i),$$

где $Stages_i = \{Stage_{ij}\}$ – вершины, представляющие собой вычислительные стадии (совокупности одинаковых и независимо выполняемых наборов операций

над различными частями входных данных); $DataStorages_i' \subseteq DataStorages$ – вершины-хранилища данных; $Precedences_i = \{(u,v) \mid u,v \in DataSources \cup Stages_i\}$ – множество дуг, задающих отношения зависимости по данным; $Volumes_i : Precedences_i \to N \cup \{0\}$ – отображение, определяющее объем данных, которые пересылаются по каждой дуге.

Вычислительная стадия $Stage_{ij}$ формализуется в виде кортежа следующего вида:

$$Stage_{ij} = (NTasks_{ij}),$$

где $NTasks_{ij}$ – количество вычислительных задач над различными частями одних и тех же наборов входных данных, получаемых с другой стадии или из хранилища. В конце каждой стадии обязательно выполняется синхронизация вычислительных задач.

Предложенный подход позволяет моделировать Map-Reduce приложения [3], в этом случае вычислительные стадии Job_i могут быть представлены в виде множества из двух стадий:

$$Stages_i = \{Map_i, Reduce_i\}.$$

Здесь Map_i включает в себя вычислительные задачи по выполнению загрузки и отображения данных, а $Reduce_i$ – задания по их редукции и сохранению результатов.

Также предложенная модель позволяет учитывать обработку данных (выполнение трансформаций и действий) над наборами RDD (Resilient Distributed Dataset) в библиотеке Spark [4]. В этом случае, $Stages_i$ может включать в себя типовые трансформации, например: map (отображение), reduce (редукцию), filter (фильтрация), groupByKey (группировка), union (объединение), join (соединение), sortByKey (сортировка) и др.

Данная модель также может учитывать динамическую составляющую выполнения приложений, в частности, может собираться статистика их выполнения на различных уровнях (с помощью стандартных инструментов Hadoop или Spark).

На уровне всего приложения App, задания Job_i и вычислительной стадии $Stage_{ij}$:

а) $T_{exec}(App)$, $T_{exec}(Job_i)$, $T_{exec}(Stage_{ij})$ – реальное время выполнения;

б) $U(App)$, $U(Job_i)$, $U(Stage_{ij})$ – средняя загрузка вычислительных ядер;

в) $RAM(App)$, $RAM(Job_i)$, $RAM(Stage_{ij})$ – пиковый размер суммарной потребляемой оперативной памяти за все время выполнения приложения;

г) $Disk(App)$, $Disk(Job_i)$, $Disk(Stage_{ij})$ – пиковый размер суммарной потребляемой дисковой памяти за все время выполнения приложения;

д) $Volume_{in}(App)$, $Volume_{in}(Job_i)$, $Volume_{in}(Stage_{ij})$ и $Volume_{out}(App)$, $Volume_{out}(Job_i)$, $Volume_{out}(Stage_{ij})$ – соответственно суммарные объемы входных и выходных данных.

Знание данных значений имеет большое значения для:

а) алгоритмов планирования выполнения облачных приложений – подбор наиболее подходящих по ресурсам виртуальных машин для выполнения вычислительных задач отдельных стадий, уменьшения окон в расписании за счет более реальных оценок времени выполнения приложений и их компонентов;

б) алгоритмов масштабирования вычислительных ресурсов – для запуска новых виртуальных машин при возрастании нагрузки на вычислительный пул и остановки части машин – при ее снижении.

Далее рассмотрим подходы к прогнозированию данных значений.

Для уровня всего приложения App обозначим вектор прогнозируемых значений:

$$Y^{App} = (T_{exec}(App), U(App), RAM(App), Disk(App), Volume_{out}(App)) . \quad (1)$$

Прогнозирование будет осуществляться на основе следующих параметров, собираемых для App:

а) $ExecFile$ – имя исполняемого файла приложения;

б) $User$ – имя пользователя, запускающего приложение;

в) $ArrivedTime$ – время поступления задачи в очередь;

г) $InputDataSize$ – размер входных данных;

д) $Resources = (r_1, r_2, ..., r_n)$ – вектор признаков ресурсов (виртуальных машин), используемых для выполнения приложения. Здесь $r_i \in N \cup \{0\}$ – количество виртуальных машин i-го типа конфигурации.

Обозначим вектор данных признаков в виде X^{App}.

Возникает задача построения модели машинного обучения M^{App}, которая способна предсказывать Y'^{App} по X^{App}:

$$Y'^{App} = M^{App}(X^{App}).$$

Это задача регрессии. Для построения данной модели необходимо подготовить набор обучающих размеченных данных (обучение с учителем):

$$X_L^{App} = \{(X_i^{App}, Y_i^{App})\}.$$

Его формирование может производиться автоматически за счет собираемой статистики предыдущих запусков работы приложений.

Для решения данной задачи могут быть использованы:

а) глубокие нейронные сети – Deep Neural Networks;

б) метод опорных векторов – Support Vector Regression;

в) логистическая регрессия – Logistic Regression;

г) решающие деревья – Decision Tree Regression;

д) бустинг деревьев – Tree Boosting;

в) ансамблевые варианты, комбинирующие результаты данных методов.

При недостаточном размере набора X_L^{App} или его неполноте (запускается совершенно новая задача), могут быть использованы эвристики для получения первичных оценок сверху для прогнозируемых параметров.

На уровне задания Job_i прогнозирование может осуществляться с помощью системы массового обслуживания, которая может быть реализована на базе дискретного событийно-управляемого симулятора QN:

$$Y_i'^{Job} = QN(Job_i), \quad (2)$$

где $Y_i'^{Job}$ – вектор прогнозируемых значений, аналогичный вектору Y'^{App} (см. формулу (1)).

Данный симулятор должен имитировать работу разрабатываемой платформы для обработки больших данных в части работы виртуальных машин и выполнения облачных приложений. При этом он должен полностью реализовывать все разрабатываемые алгоритмические решения, включая алгоритмы планирования облачных приложений и масштабирования вычислительных ресурсов. В своей работе симулятор опирается на прогнозируемые значения, предсказанные для отдельных стадий.

Кроме того, данный симулятор может быть модифицирован для прогнозирования значений, на уровне приложения, поэтому формула (2) может быть уточнена следующим образом:

$$(Y^{App}, Y'^{Jobs}) = QN'(App),$$

где $Y'^{Jobs} = (Y_1'^{Jobs}, ..., Y_{|Jobs|}'^{Jobs})$ - вектор прогнозных значений для отдельных задач, QN' – модифицированная система массового обслуживания.

На уровне стадии $Stage_{ij}$, если она представляет собой простую или типовую операцию над данными (например, трансформацию над RDD в Spark), возможно использование методов машинного обучения, аналогично уровню приложения. При этом будет составляться вектор признаков X_{ij}^{Stage}, а обученная регрессионная модель M^{Stage} будет вычислять вектор предсказываемых значений:

$$Y_{ij}'^{Stage} = M^{Stage}(X_{ij}^{Stage}).$$

На следующем этапе исследования планируется провести сравнение эффективности работы предложенных методов прогнозирования параметров на разных уровне с использованием реально собранных данных. При этом для моделей машинного обучения должна использоваться техника кросс-валидации (cross validation). Также предполагается подстройка гиперпараметров моделей машинного обучения за счет использования алгоритма grid search.

Достоинства предложенной модели приложений для обработки больших данных:

а) учет параллелизма на уровне заданий и отдельных стадий;

б) совмещение параллелизма по задачам (на уровне приложения - последовательное выполнение заданий, на уровне задания – ориентированный ацикличный граф стадий) и по данным (в задачах на уровне отдельной стадии);

в) возможность моделировать современные приложения для обработки больших данных, включая Map-Reduce (приложения Hadoop) и Spark;

г) возможность учитывать не только структурные, но и динамические параметры приложений.

Предложенные методы прогнозирования могут быть использованы для получения приблизительных оценок характеристик приложений для обработки больших данных с учетом выделяемых ресурсов.

Работа выполнена при поддержке РФФИ (проекты №18-07-01446 и № 18-37-00460).

Список литературы

1 Большие данные (Big Data) [Электронный ресурс] / TADVISER, 2017. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Большие_данные_(Big_Data)

2 HDFS Architecture Guide [Электронный ресурс] / The Apache Software Foundation, 2018. – Режим доступа: https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html

3 Apache Hadoop [Электронный ресурс] / The Apache Software Foundation, 2018. – Режим доступа: view-source:https://hadoop.apache.org/

4 RDD Programming Guide [Электронный ресурс] / The Apache Software Foundation, 2018. – Режим доступа: https://spark.apache.org/docs/latest/rdd-programming-guide.html#basics

ОБЗОР ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Прокофьев А. В.
Оренбургский государственный университет

Применение криптографических методов и средств защиты информации в современных цифровых технологиях становится неотъемлемой частью многих сфер жизни нашего общества, поэтому проблемы криптостойкости и шифров являются актуальными и важными в современной криптографии.

Известно, что все последовательности, возникающие в криптографических приложениях, периодичны. Любую периодическую последовательность можно рассматривать как линейную рекуррентную последовательность, пусть и очень большого порядка.

С точки зрения криптографии все современные компиляторы хоть и обладают собственной реализацией генератора псевдослучайных последовательностей, но они не являются пригодными.

Основная проблема – это сложность генерации последовательности псевдослучайных чисел на компьютере в том, что вычислительные машины детерминированы по своей сути. Компьютер может находиться только в конечном количестве состояний (количество состояний огромно, но все-таки конечно). Таким образом, любое устройство генерации случайных чисел по определению периодично, то есть не случайно.

В настоящее время генерация псевдослучайных чисел широко востребована в разных приложениях, будь то функции случайных чисел в программировании, помогающие в прикладных задачах, статистических исследованиях, лотереях либо военных целях.

Генераторы псевдослучайных последовательностей. Случайные числа требуются в криптографии очень часто. Симметричный ключ шифрования должен выбираться случайным образом. При генерации ключей для асимметричной криптосистемы необходимо иметь достаточно большой объем случайных данных.

В компьютере, в общем случае, нет хорошего источника случайности, способного выдавать значительные объемы истинно случайных данных. Поэтому в криптографии находят широкое применение так называемые генераторы псевдослучайных чисел (ГПСЧ).

Существуют истинно случайные генераторы. Примером такого может быть, например, игральный куб без смещённого центра тяжести.

Линейный регистр сдвига с обратной связью. Большинство реальных поточных шифров основано на регистрах сдвига с обратной связью (РСОС). Регистр сдвига применяют для генерации ключевой последовательности. Регистр сдвига с обратной связью показан на рисунке 1 и состоит из двух частей: регистра сдвига и функции обратной связи.

Рисунок 1 – регистр сдвига с обратной связью

Регистр сдвига представляет собой последовательность битов. Количество битов определяется длиной сдвигового регистра. Если длина равна n битам, то регистр называется *n*-битовым регистром сдвига.

Когда нужно извлечь бит, все биты регистра сдвига сдвигаются вправо на 1 позицию. Новый крайний левый бит является функцией всех остальных битов регистра.

На выходе регистра оказывается один, обычно младший значащий бит. Периодом регистра называется длина получаемой последовательности до начала ее повторения.

Простейшим видом регистра сдвига с обратной связью является регистр сдвига с линейной обратной связью (РСЛОС). Обратная связь представляет собой логическую операцию «ИЛИ» (XOR) некоторых битов регистра - эти биты называются отводной последовательностью. Регистр сдвига с линейной обратной связью показан на рисунке 2.

РСЛОС (n - битовый) может находиться в одном из 2^n-1 внутренних состояний. Это означает, что теоретически такой регистр может генерировать псевдослучайную последовательность с периодом 2^n-1 битов.

Число внутренних состояний и период равны 2^n-1, потому что заполнение РСЛОС нулями приведет к тому, что сдвиговый регистр будет выдавать бесконечную последовательность нулей, что абсолютно бесполезно.

Только при определенных отводных последовательностях РСЛОС циклически пройдет через все 2^n-1 внутренних состояний. Такие РСЛОС имеют максимальный период. Получившийся результат называется М-последовательностью. Для того чтобы конкретный РСЛОС имел максимальный период, многочлен, ассоциированный с отводной последовательностью, должен быть примитивным по модулю 2 — то есть не раскладываться на произведение двоичных многочленов меньшей степени.

Регистр сдвига представляет собой электронную схему, позволяющая вырабатывать последовательность, определяемую линейным рекуррентным уравнением. Схема состоит из двух элементов. Один из элементов называется сумматор, второй – задержкой. Сумматор имеет два входа и один выход. Задержка имеет один вход и один выход.

Если на вход сумматора подаются два одинаковых сигнала, то на выход подается 0, в противном случае 1. Сумматор реализует двоичную функцию.

Если на вход задержки подается какой-нибудь сигнал, то на выход идет тот же сигнал. Сумматор и задержка показаны на рисунке 2.

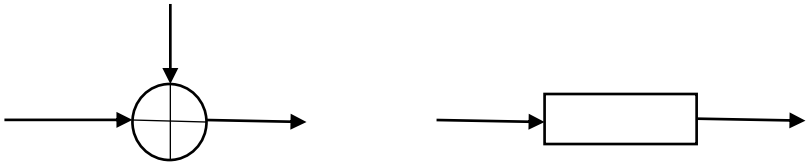


Рисунок 2 – элементы регистра сдвига: сумматор и задержка

Пример. Уравнению (1.1) построена схема регистра сдвига, изображенная на рисунке 2.

$$\partial_{x+5} = \partial_x + \partial_{x+3}, \qquad (1.1.)$$

где - $\partial_0 = 1$;
$\partial_1 = 0$;
$\partial_2 = 0$;
$\partial_3 = 0$;
$\partial_4 = 0$.

Периодическая последовательность: 1000101011101100000… с примитивным периодом 31.

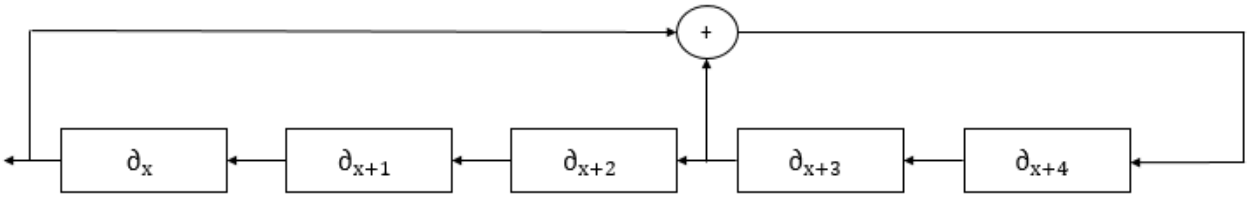


Рисунок 3 – регистр сдвига с линейной обратной связью

РСЛОС являются хорошими генераторами псевдослучайных последовательностей, но они обладают некоторыми нежелательными неслучайными свойствами. Для РСЛОС длины равной n, внутреннее состояние представляет собой предыдущие n выходных битов генератора. Даже если схема обратной связи хранится в секрете, она может быть определена по $2n$ выходным битам генератора с помощью алгоритма Берлекэмпа-Мэсси.

Схему обратной связи также можно модифицировать. При этом генератор не будет обладать большей криптостойкостью, но его будет легче реализовывать программно. Вместо использования для генерации нового крайнего левого бита битов отводной последовательности выполняется XOR каждого бита отводной

последовательности с выходом генератора и замена его результатом этого действия, затем результат генератора становится новым левым крайним битом. Такая модификация схемы обратной связи называется – конфигурация Галуа.

Линейный конгруэнтный метод был предложен Д. Г. Лемером в 1949 году [1]. Цель метода заключалась в вычислении последовательности случайных чисел X_n, полагая по формуле (1.2):

$$X_{n+1} = (aX_n + c) \bmod m, \qquad (1.2)$$

где m – модуль (натуральное число, относительно которого вычисляет остаток от деления; $m \geq 2$), a – множитель ($0 \leq X_0 < m$).

Эта последовательность называется линейной конгруэнтной последовательностью. Например, для $m = 10$, $X_0 = a = c = 7$ получим последовательность 7,6,9,0,7,6,9, 0, ….

Линейная конгруэнтная последовательность, определенная числами m, a, c и X_0, периодична с периодом, не превышающим m. При этом, длина периода равна m тогда и только тогда, когда [3]:

1. Числа c и m взаимно простые;

2. $a – 1$ кратно p для каждого простого p, являющегося делителем m;

3. $a – 1$ кратно 4, если m кратно 4.

Наличие этого свойства для случая $m = 2^e$, где e – число битов в машинном слове, было доказано М. Гринбергом [4]. Наличие этого свойства для общего случая и достаточность условий были доказаны Т. Е. Халлом и А. Р. Добеллом [5].

Метод генерации линейной конгруэнтной последовательности при $c = 0$ называют мультипликативным конгруэнтным методом, а при $c \neq 0$ – смешанным конгруэнтным методом. При $c = 0$ генерируемые числа будут иметь меньший период, чем при $c \neq 0$, но при определенных условиях можно получить период длиной $m – 1$, если m – простое число. Тот факт, что условие $c \neq 0$ может приводить к появлению более длинных периодов, был установлен В. Е. Томсоном и независимо от него А. Ротенбергом [2]. Чтобы гарантировать максимальность цикла повторения последовательности при $c = 0$, необходимо в качестве значения параметра m выбирать простое число. Самым известным генератором подобного рода является так называемый минимальный стандартный генератор случайных чисел, предложенный Стивеном Парком и Кейтом Миллером в 1988 году. Для него $a = 16807$, а $m = 2147483647$ [6] [7].

Наиболее часто практикуемым методом генерации последовательностей псевдослучайных чисел является смешанный конгруэнтный метод.

При выборе числа m необходимо учитывать следующие условия:

1) число m должно быть довольно большим, так как период не может иметь больше m элементов;

2) значение числа m должно быть таким, чтобы $(aX_n + c) \bmod m$ вычислялось быстро.

На практике при реализации метода исходя из указанных условий чаще всего выбирают $m = 2^e$, где e – число битов в машинном слове. При этом стоит учитывать, что младшие двоичные разряды сгенерированных таким образом случайных чисел демонстрируют поведение, далёкое от случайного, поэтому рекомендуется использовать только старшие разряды. Подобная ситуация не возникает, когда $m = w \pm 1$, где w – длина машинного слова. В таком случае младшие разряды X_n ведут себя так же случайно, как и старшие [2]. Выбор множителя a и приращения c, в основном, обусловлен необходимостью выполнения условия достижения периода максимальной длины.

Преимуществами линейных конгруэнтных генераторов являются хорошие статистические свойства, простота их реализации и быстрота. Однако их нельзя использовать в криптографии, так как они не являются криптостойкими, что связано в том числе с «решетчатостью» их структуры. То есть, имея последовательность чисел, полученную таким генератором, оппонент может восстановить параметры генератора, затратив минимум усилий.

Тем не менее, линейные конгруэнтные генераторы являются полезными для не криптографических приложений. Например, в моделировании или в игровых приложениях.

Генератор Фибоначи. Последовательность Фибоначчи была хорошо известна в древней Индии, где она применялась в метрических науках (просодии, другими словами - стихосложении), намного раньше, чем она стала известна в Европе.

В отличие от линейного конгруэнтного генератора в правую часть рекуррентного соотношения обобщенного генератора Фибоначчи входит два члена предшествующей последовательности. Другое название этого генератора «запаздывающий генератор Фибоначчи» (LFG). Известны разные схемы использования метода Фибоначчи с запаздыванием. Один из широко распространённых «Фибоначиевых» датчиков основан на рекуррентной формуле (1.3):

$$k_i = \begin{matrix} k_{i-a} - k_{i-b}, \text{если } k_{i-a} \geq k_{i-b} \\ k_{i-a} - k_{i-b} + 1, \text{если } k_{i-a} < k_{i-b} \end{matrix}, \qquad (1.3)$$

где - k_i- вещественное число диапозона [0,1];
a,b – параметры генератора, вещественные числа

Для оптимальной работы датчику «Фибоначи» требуется знать max{a,b} предыдущих сгенерированных случайных чисел.

Для достижения цели программной реализации, хранения сгенерированных случайных чисел, необходим некоторый объем памяти, зависящих от вышеуказанных параметров a и b из формулы (1.1).

Параметры должны быть протестированы на качество. Качество получаемых случайных чисел зависит от значения константы.

Чем оно больше, тем выше размерность пространства, в котором сохраняется равномерность случайных векторов, образованных из полученных случайных чисел. В то же время с увеличением величины константы a увеличивается объём используемой алгоритмом памяти.

Генераторы ПСЧ, основанные на методе Фибоначчи с запаздыванием, использовались для целей криптографии. Кроме того, они применяются в математических и статистических расчетах, а также при моделировании случайных процессов. Генератор ПСЧ, построенный на основе метода Фибоначчи с запаздыванием, использовался в широко известной системе Matlab.

Генератор с квадратичным остатком. Для достижения целей криптографии в 1986 году предложен генератор с квадратичным остатком.

Суть генератора заключается в следующем:

1) Изначально выбираются два больших простых числа p и q. Числа p и q должны быть оба сравнимы с 3 по модулю 4;

2) Далее вычисляется целое число Блюма:

$$M = p * q \tag{1.4}$$

3) Далее выбирается другое случайное целое число x, взаимно простое с M (то есть не имеющее общих делителей, кроме единицы).

4) Далее считают стартовое число генератора (1.5):

$$x_0 = x^2 mod\ M \tag{1.5}$$

На каждом (n-м) шаге работы генератора вычисляется:

$$x_{n+1} = x_n^2\ mod\ M \tag{1.6}$$

Результатом n-го шага является один младший бит числа - (x_{n+1}). Так же в качестве результата принимают бит чётности, то есть количество единиц в двоичном представлении элемента. Если количество единиц в записи числа четное – бит четности принимается равным 0, нечетное – бит четности принимается равным.

Безопасность алгоритма BBS реализована на сложности разложения большого числа M на несколько множителей. Если M достаточно большое, то его можно даже не держать в секрете. Или держать до тех пор, пока M не разложено на множители, никто не сможет предсказать выход генератора ПСЧ.

Это связано с тем, что задача разложения чисел на множители вида:

$$n = p * q, \tag{1.7}$$

где – p, q – простые числа.

Является вычислительно очень трудной, если знать только n, а p и q - большие числа, состоящие из нескольких десятков или сотен бит – задача факторизации.

Можно доказать, что хакер, зная некоторую последовательность, сгенерированную генератором BBS, не сможет определить ни предыдущие до нее биты, ни следующие. Генератор BBS непредсказуем. Это свойство очень полезно для целей криптографии, и оно также связано с особенностями разложения числа M на множители.

Один из существенных недостатков генератора является то, что он недостаточно быстр, что не позволяет использовать его во многих областях. Например, при вычислениях в реальном времени, а также при потоковом шифровании.

Главное достоинство генератора - алгоритм выдает действительно хорошую последовательность псевдослучайных чисел с большим периодом (при соответствующем выборе исходных параметров), что позволяет использовать его для криптографических целей при генерации ключей для шифрования.

Инверсный конгруэнтный метод был предложен Эйченауэром и Лехном в 1986 году [4] как замена линейному конгруэнтному методу, не обладающему решётчатой структурой [5].

Данный метод состоит в вычислении последовательности случайных чисел x_n в кольце вычетов по модулю натурального числа n.

Основным отличием от линейного метода является использование при генерации последовательности числа, обратного к предыдущему элементу, вместо самого предыдущего элемента.

Параметрами генератора являются [6]:

seed – соль,

a – множитель ($0 \le a < n$),

b – приращение ($0 \le b < n$).

В случае простого n значение членов последовательности задается в виде (1.7) и (1.8):

$$x_0 = seed, \tag{1.7}$$

$$x_{i+1} \equiv (ax_i^{-1} + b) \bmod n. \tag{1.8}$$

Параметры подбираются таким образом, чтобы (1.9) и (1.10):

$$(seed, n) = 1; \tag{1.9}$$

$$(a, n) = 1. \tag{1.10}$$

Последовательность, формируемая инверсным конгруэнтным генератором, определенным числами a, b и n, имеет максимальный период, равный $n + 1$, когда многочлен $f(x) = x^2 - cx - a$ обладает следующими свойствами:

1. $x^{p+1} \bmod f(x)$ равняется отличной от нуля константе;

2. $x^{(p+1)/q} \bmod f(x)$ имеет степень 1 для каждого простого q, делящего значение $p + 1$.

Значение $p + 1$ является исключительно теоретическим, так как получается в предположении, что $0^{-1} = \infty$ и $\infty^{-1} = 0$. На практике обычно полагают $0^{-1} = 0$, в этом случае максимальный период равен p.

В качестве примера рассмотрим инверсный конгруэнтный генератор с параметрами $n = 5$, $a = 2$, $b = 3$, $seed = 1$. Он генерирует последовательность {1,0,3,2,4,1, …} в кольце F_5, где числа 1 и 4, а также 2 и 3 обратны друг другу. В данном примере многочлен $f(x) = x^2 - 3x - 2$ неприводимом в F5[x] и числа 0,1,2,3,4 не являются его корнями, благодаря чему период максимален и равен $n = 5$.

В инверсных конгруэнтных генераторах отсутствует «решетчатая» структура.

Список литературы

1 Дональд Э. Кнут. Искусство программирования. — 3-е изд. — М.: Вильямс, 2000. — Т. 2. Получисленные алгоритмы. — 832 с.

2 Л. Бараш Алгоритм AKS проверки чисел на простоту и поиск констант генераторов псевдослучайных чисел // Безопасность информационных технологий. — 2005. — № 2. — с. 27-38.

3 Stephen K. Park and Keith W. Miller Random Number Generators: Good Ones Are Hard To Find. — 1988. — № 2. — с. 1192-1201.

4 Бакнелл Д.М. Фундаментальные алгоритмы и структуры данных в Delphi.Библиотека программиста. // Delphi Informant Magazine. — 2002.

5 Дональд Кнут. Том 2. Получисленные методы // Искусство программирования. Указ. соч. — с. 21—37.

6 M. Greenberger, Method in randomness, Comm. ACM 8 — 1965 — с. 177—179.

7 T.E. Hull and A.R. Dobell «Random Number Generators», SIAM Review 4-3 — 1962 — с. 230-254.

ИСПОЛЬЗОВАНИЕ МУЛЬТИМЕДИА ТЕХНОЛОГИЙ В ПРОЦЕССЕ ОБУЧЕНИЯ КАК ФАКТОР ПОВЫШЕНИЯ УРОВНЯ ОБРАЗОВАНИЯ СТУДЕНТОВ

Ряполова Е.И., канд. пед. наук, доцент
Оренбургский государственный университет

Глобальная информатизация образования толкает преподавателей к использованию информационных и мультимедиа технологий в образовании. Возрастает значимость использования гиперссылочных и электронных учебных пособий и методических материалов в образовательном процессе.

Необходимость за короткие сроки изучить большой объема теоретического материала студентами предполагает организацию обучения по узловым вопросам изучаемой дисциплины. Одной из современных тенденций развития образования - переход к моделирующему обучению, которое позволяет ориентировать студента на личностный рост, саморазвитие и формирование ключевых компетентностей.

Данная тенденция в образовании требует осознанного подхода к построению курса обучения, отбору содержания и структуре.

Проблемам оптимизации и интенсификации процесса обучения занимались исследователи : А.А. Крашенников, Ю.К. Бабанский, В.В. Давыдов, С.И. Архангельский, А.А. Вербицкий, В.П. Беспально. В работах В.С. Леднева, Г.Н. Серинова, М.Н. Скаткина, В.В. Шапкина отражены подходы к структурированиию содержания образования. Использованием информационных технологий в процессе образования занимались: Л.Х. Зайнутдинова, В.А. Красильникова, Е.С. Полат, И.В. Роберт и другие.

Представление и деление учебной дисциплины на блоки или модули зачастую происходит на основе субъективных представлений разработчиков курсов и не основываются на сложности излагаемого материала [1,2].

В данной статье представлена разработка электронного гиперссылочного учебного пособия «Информатика» которое разрабатывалось:

- для организации различных видов тестирования знаний студентов;
- для организации самостоятельного изучения дисциплины;
- как дополнительное средство обучения для студентов.

Разработанное гиперссылочное пособие обладает рядом достоинств: учитывает межпредметные связи, доступность, простота использования, системность, наглядность, возможность изучение материала в домашних условиях, индивидуальный темп изучения материала .

Методическая и практическая ценность разработанного электрогенного учебного пособия «Информатика» заключается в том, что использование информационных и мультимедийных технологий в образовательном процессе дают значительные дидактические преимущества по сравнению с традиционной формой образования, создают наглядное представление информации, способствуют лучшему восприятию теоретического материала, направлены на

самостоятельное изучения материала и подразумевают индивидуальный темп работы.

Гиперссылочное электронное учебное пособие «Информатика» включает в себя курс лекций, лабораторные работы, контрольные вопросы, интерактивное тестирование и список литературы. Переключаться между элементами пособия можно с помощью интерактивного меню. Курс лекций содержит 18 тем. На любой из открытых лекций в левой части экрана существует меню навигации между темами (рисунок 1).

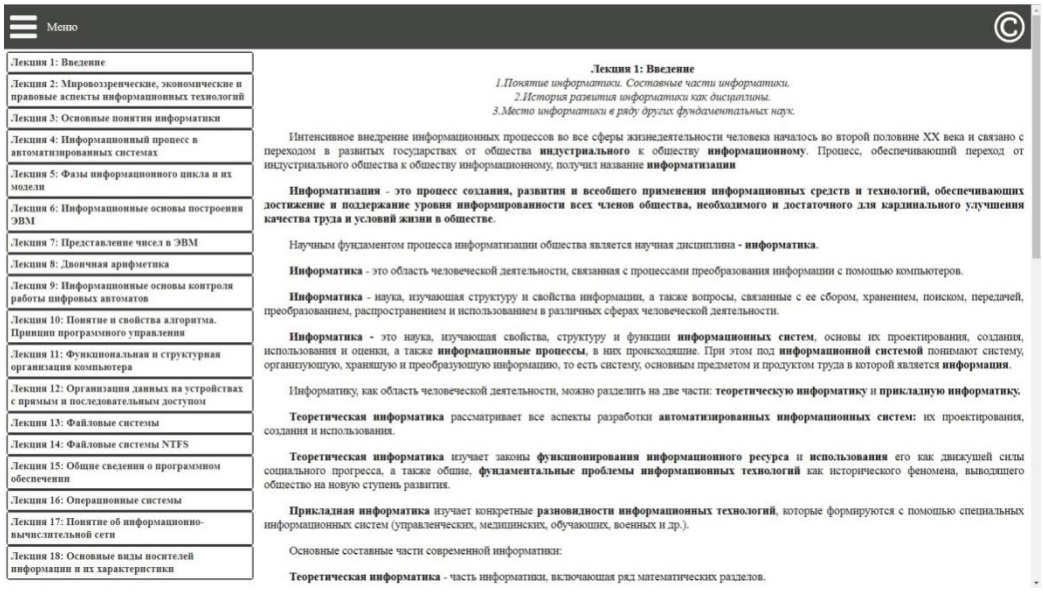


Рисунок 1 – Экранная форма оформления лекций электронного гиперссылочного учебного пособия

Лекции сопровождаются графическим материалом и пояснениями (рисунок 2).

Все сигналы могут быть подразделены на **периодические** и **непериодические**. **Периодическим называется сигнал**, **значения которого повторяются через определенные равные промежутки времени**, **называемые периодом повторения сигнала** (***T***), или просто **периодом**. Для непериодического сигнала это условие не выполняется.

Простейшим периодическим сигналом является гармоническое колебание: ***s(t)=Ssin(ωt),*** где ***S, ω-****соответственно амплитуда и угловая частота колебания, равная*

$$\omega = 2\pi f = 2\pi / T$$

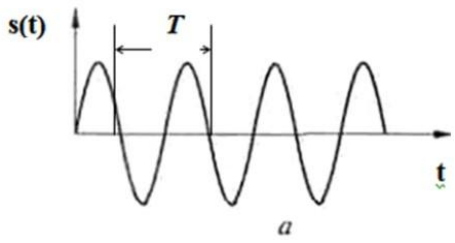


Рисунок 7 – График простейшего переиодического сигнала

Другим примером периодического сигнала является последовательность прямоугольных импульсов (б). Можно показать, что такая последовательность импульсов является результатом сложения большого числа гармонических колебаний (в общем случае - бесконечного) с разными амплитудами, частотами и начальными фазами.

Рисунок 2 – Экранная форма лекции электронного гиперссылочного учебного пособия

Всего в методическом пособии 9 лабораторных работ, 4 из которых являются дополнительными, у студента есть возможность проверить себя после решения одной из лабораторных с помощью контрольных вопросов. Также существует 9 интерактивных тестов, вопросы в которых составлены на основе курса лекций (рисунок 3).

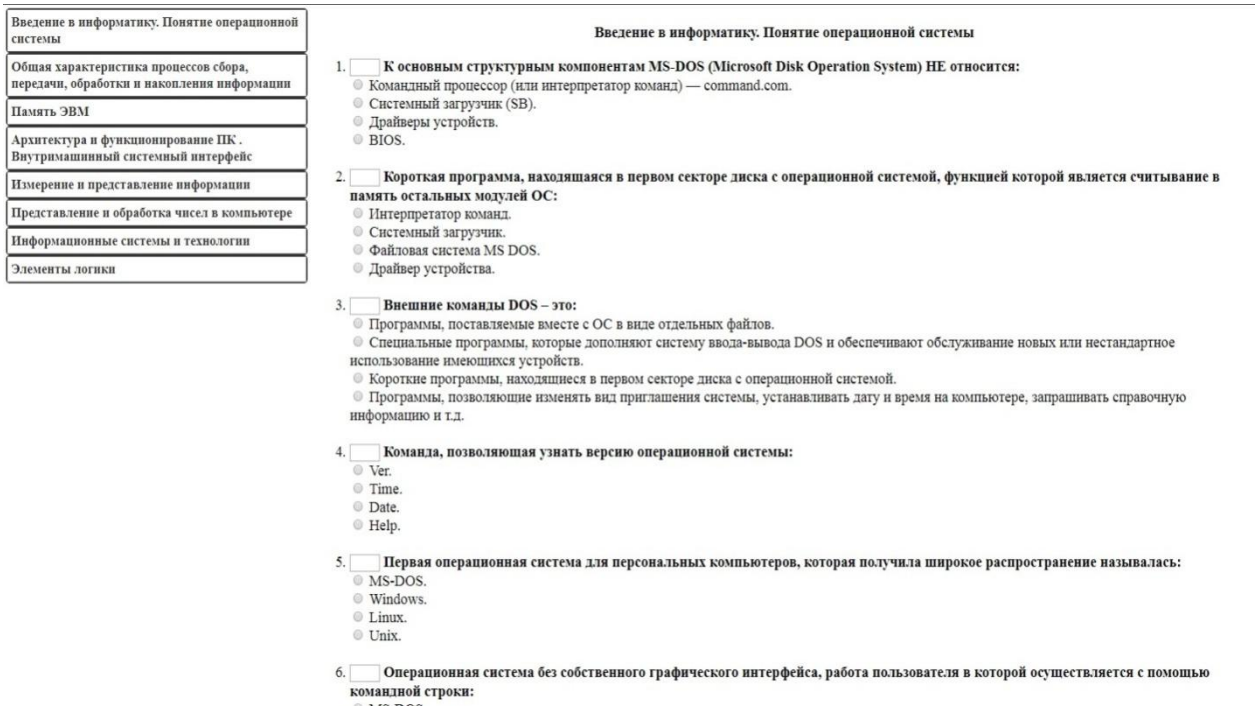


Рисунок 3 – Экранная форма оформления интерактивного тестирования

В ходе изучения дисциплины «Информатика» студенты могут пройти составленные тесты для проверки усвоенных знаний.

Электронное гиперссылочное учебное пособие «Информатика» разработано как дополнительное информационное средство для сопровождения процесса проведения занятий по дисциплине «Информатика» для студентов направления подготовки 10.03.01 «Информационная безопасность», так же данное учебное пособие может быть использовано для самостоятельного изучения дисциплины и для подготовки к выполнению лабораторных работ.

В заключение можно отметить, что разрабатывать электронные учебные курсы в условиях личностно ориентированного обучения необходимо выделив общее и особенное в процессе учения - преподавания. Студенты в процессе такого обучения учатся целеполаганию, критическому мышления, саморазвитию, планированию, контролю и оценке своей деятельности. В процессе обучения с использование электронного учебного курса студенты осваивают новый способ общения с преподавателем. Преподаватель в данном случае управляет познавательной деятельностью студентов индивидуально и целенаправленно. Таким образом, построенный процесс обучения в большей степени способствует развитию познавательной самостоятельности студентов в процессе поисковой

деятельности, мобильности и гибкости действий студентов по достижению поставленных целей, самостоятельному распределению времени на изучение материала, направленности на саморазвитие.

Список литературы

1 Чошанов М.А. Гибкая технология проблемно-модульного обучения: Методическое пособие.- М.: Народное образование, 1996.- 160с.

2 Эрдниев П.М. Укрупнение дидактических единиц как технология обучения. - Ч.1.- М.: Просвещение, 1992.- 175с.

3 Prokopenko J., White J., Bittel L, Eckles R. Modular programme for supervisoru development. Switzerland, Genewa: Introduction and Trainers Guide, 1981. Vol. 1-5

4 Russe LG.D. ModuLsar Instruction // A Guid for Pesign. Minneapolis: Burges Publ, 1974.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ПОСТРОЕНИЯ ДЕРЕВА ПРИНЯТИЯ РЕШЕНИЙ

Симченко Н. Н., канд. пед. наук, доцент
Оренбургский государственный университет

Алгоритмы построения дерева принятия решений являются одним из инструментов решения задач классификации и прогнозирования. Для построения дерева решений используется метод итераций: при построении вершины дерева выбирается признак, оптимальным образом удовлетворяющий определенному критерию ветвления. По значениям этого признака осуществляется ветвление, далее указанная процедура повторяется для каждой из ветвей. Построенные деревья могут отличаться как по структуре, так и по своим качествам в зависимости от выбранного признака. Задача состоит в построении наиболее простого дерева с высокой обобщающей способностью.

Для решения такой задачи – поиска наилучшего баланса между размером дерева и его качеством, используются различные методы редукции дерева. Цель состоит в создании модели, которая будет предсказывает значение целевой переменной на основе нескольких переменных на входе. В связи с необходимостью обработки огромных массивов неструктурированной информации создаются методы семантического анализа текстов и технологии работы с «большими данными», в результате активно распространяется предсказательное моделирование [2].

В рамках данного исследования была поставлена задача проанализировать зависимость уровня подготовки учителя от места проживания, категории, стажа работы и образования. Для этого была спроектирована структура данных, основанная на результатах тестирования, которое было проведено для определения уровня предметной составляющей профессиональной компетенции учителя информатики. Для контроля знаний в тест были включены вопросы двух уровней сложности: низкий и высокий. Содержание тестовых вопросов отражало все содержательные линии школьного предмета «Информатика» в полном соответствии с ФГОС полного (среднего) образования. В качестве выходного определен атрибут –Уровень, показывающий уровень подготовки учителя, принимающий значение «высокий», если учитель, верно ответил на вопросы высокого уровня сложности и значение «низкий», если учитель ответил верно на вопросы на распознавание, которые представлены тестами с выборочными ответами [3].

Для построения дерева решений был рассмотрен следующий фрагмент хранилища данных, полученный экспериментально (таблица 1).

Таблица 1 – Хранилище данных

Образование	Район/Город	Категория	Стаж	Уровень
Профильное	Город	Высшая	>20	высокий
Профильное	Районный	Высшая	>20	высокий

	центр			
Образование	Район/Город	Категория	Стаж	Уровень
Непрофильное	Город	Первая	<5	низкий
Непрофильное	Город	Нет	<5	низкий
Профильное	Районный центр	Первая	11-20	высокий
Непрофильное	Город	Первая	<5	низкий
Профильное	Районный центр	Первая	5-10	высокий
Непрофильное	Город	Первая	<5	низкий
Непрофильное	Город	Нет	<5	низкий
Непрофильное	Город	Нет	<5	низкий
Профильное	Областной центр	Высшая	>20	высокий
Непрофильное	Областной центр	Первая	<5	низкий
Непрофильное	Город	Первая	<5	низкий
Профильное	Город	Первая	5-10	высокий
Непрофильное	Районный центр	Нет	<5	низкий
Профильное	Город	Первая	5-10	низкий
Непрофильное	Районный центр	Нет	<5	низкий
Профильное	Село	Первая	5-10	высокий
Непрофильное	Город	Нет	<5	низкий
Профильное	Областной центр	Высшая	>20	высокий

Общая схема построения дерева принятия решений по тестовым примерам выглядит следующим образом:

1) Выбирается очередной атрибут и помещается в корень.

2) Для всех значений выбранного атрибута делается следующее:

- из тестовых примеров оставляются только те, у которых значение выбранного атрибута равно выбранному значению;
- в этом потомке, при помощи рекурсии, строится дерево.

Основной задачей является задача выбора основного атрибута. Есть различные способы выбора атрибута. В рамках данного исследования рассмотрены два алгоритма построения дерева принятия решений: алгоритм ID3 и алгоритм C4.5.

Алгоритм ID3, где выбор атрибута происходит на основании прироста информации (англ. Gain), либо на основании индекса Гини. Алгоритм C4.5 (улучшенная версия ID3), где выбор атрибута происходит на основании нормализованного прироста информации. Алгоритм ID3 строит решающее

дерево, в котором с каждым узлом ассоциирован атрибут, являющийся наиболее информативным среди всех атрибутов, еще не рассмотренных на пути от корня дерева [1].

В исследовании была разработана программная реализация алгоритма ID3, выбран язык программирования C#, среда разработки Microsoft Visual Studio 2012. Для хранения информации об атрибутах в программе описана структура attributes:

```
struct attributes
{
   public string name;
   public string[] values;
}
```

Для хранения дерева принятия решений в программе описан класс item_tree:

```
class item_tree
{
   public attributes a;
   public int num_attr;
   public int obuch = 0;
   public string res;
   public item_tree[] children;
   public bool[] enter=new bool[count];
}
```

Для того, чтобы получить более оптимальное дерево принятия решений, нужно на каждом шаге выбирать атрибуты, которые «лучше всего» характеризуют целевую функцию. Это требование формализуется посредством понятия энтропии. На основании программной реализации алгоритма ID3 было построено дерево решений. По окончании построения дерева принятия решений, можно спрогнозировать Уровень подготовки, определив образование (профильное/непрофильное), категорию (высшая, первая, нет) и стаж. Результаты такого прогноза представлены на рисунке 2.

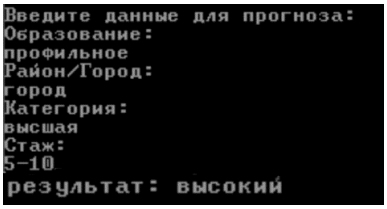


Рисунок 2 – Результат прогноза

Еще одним методом построения дерева принятия решения, является алгоритм C4.5, который представляет собой усовершенствованный вариант алгоритма ID3. Он дает возможность работать не только с категориальными атрибутами, но также с числовыми [3].

В качестве инструментария для построения дерева методом C4.5 использована аналитическая платформа Deductor. Реализованные в Deductor технологии позволяют на базе единой архитектуры пройти все этапы построения аналитической системы: от создания хранилища данных до автоматического подбора моделей и визуализации полученных результатов. В начале исходное множество данных разделяется на обучающее и тестовое, в нашем случае использовался случайный способ разбиения.

Построенное дерево, фрагмент которого показан на рисунке 3, содержит 26 листьев (правил) и 34 узла.

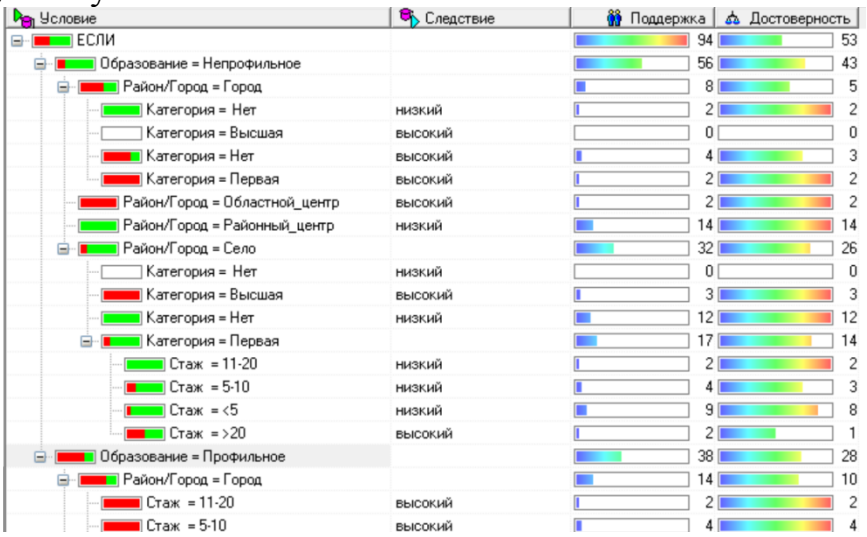


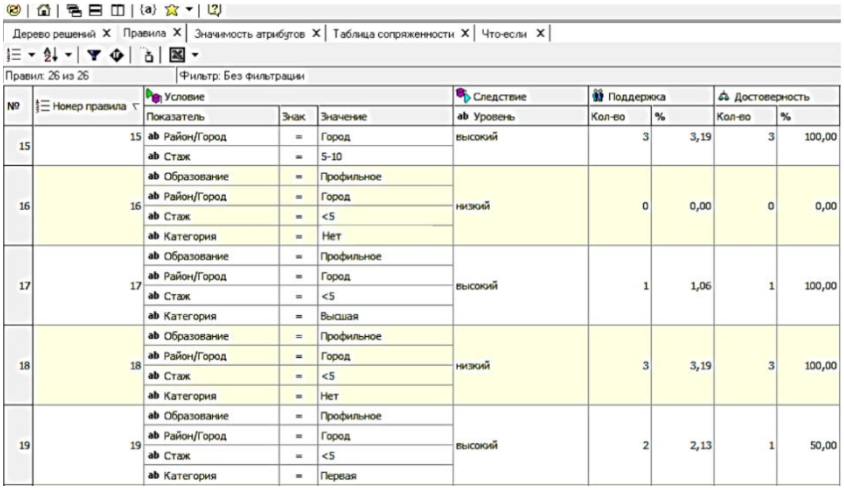
Рисунок 3– Дерево решений

Для оценки качества модели было оценено при помощи таблицы сопряженности, построенной с помощью обработчика «Дерево решений». По таблице сопряженности, представленной на рисунке 4, можно посмотреть, сколько объектов удалось классифицировать правильно.

	Классифицировано		
Фактически	высокий	низкий	Итого
высокий	42	3	45
низкий	5	49	54
Итого	47	52	99

Рисунок 4 – Таблица сопряженности для построенного дерева решений

Полученное дерево содержит в себе правила (рисунок 5), следуя которым можно спрогнозировать Уровень.



Дерево решений | Правила | Значимость атрибутов | Таблица сопряженности | Что-если

Правил: 26 из 26 | Фильтр: Без фильтрации

№	Номер правила	Условие			Следствие	Поддержка		Достоверность	
		Показатель	Знак	Значение	Уровень	Кол-во	%	Кол-во	%
15	15	Район/Город	=	Город	высокий	3	3,19	3	100,00
		Стаж	=	5-10					
16	16	Образование	=	Профильное	низкий	0	0,00	0	0,00
		Район/Город	=	Город					
		Стаж	=	<5					
		Категория	=	Нет					
17	17	Образование	=	Профильное	высокий	1	1,06	1	100,00
		Район/Город	=	Город					
		Стаж	=	<5					
		Категория	=	Высшая					
18	18	Образование	=	Профильное	низкий	3	3,19	3	100,00
		Район/Город	=	Город					
		Стаж	=	<5					
		Категория	=	Нет					
19	19	Образование	=	Профильное	высокий	2	2,13	1	50,00
		Район/Город	=	Город					
		Стаж	=	<5					
		Категория	=	Первая					

Рисунок 5 – Классификационные правила

Каждому входному атрибуту соответствует значимость – степень зависимости выходного поля от этого атрибута. Параметр Значимость тем больше, чем больший вклад вносит конкретный входной атрибут при классификации выходного поля. Фактически данный визуализатор показывает степень нелинейной зависимости между выходным и входными полями. Значимость рассчитывается на основе энтропии.

С помощью визуализатора, изображенного на рисунке 6, можно определить, насколько сильно выходное поле зависит от каждого из входных факторов. Чем больше значимость атрибута, тем больший вклад он вносит при классификации.

Целевой атрибут: Уровень

№	Номер	Атрибут	Значимость, %
1	1	Образование	31,361
2	2	Категория	30,759
3	3	Район/Город	25,774
4	4	Стаж	12,106

Рисунок 6 – Значимость атрибутов

Анализ построенного дерева принятия решений, показывает, что на уровень подготовки учителя наибольшее влияние оказывает образование (профильное/непрофильное). Проанализировав ветвь «Профильное», было выявлено, что наиболее информативным является атрибут «Стаж», если категория «Высшая», то «Уровень» – «Высокий», если «Вторая», то «Низкий».

Деревья, построенные с помощью алгоритмов ID3 и C4.5. на одном и том же наборе данных, отличаются друг от друга. Проведем анализ приведенных алгоритмов, сравнив характеристики полученных решающих деревьев.

Для исследования структуры и качества дерева принятия решений в зависимости от применяемого критерия ветвления будем использовать следующие характеристики дерева:

1) число листьев дерева;

2) глубина дерева;

3) средняя глубина листьев дерева;

4) взвешенная глубина распределения описаний обучающих объектов по листьям дерева;

5) «оптимальность» распределения обучающих объектов по листьям дерева (абсолютная разница между средней глубиной листьев дерева и взвешенной глубиной распределения описаний обучающих объектов по листьям дерева);

6) оценка качества дерева с помощью метода «leave-one-out».

Первые два свойства указывают на то, что:

– интерпретируемость решающего правила увеличивается при небольшой глубине решающего дерева;

– оценка вероятности ошибки решающего правила уменьшается с уменьшением глубины дерева;

– вероятность обнаружения неслучайной конъюнктивной закономерности выше, а ранг конъюнкций ниже, тогда, когда меньше глубина дерева.

– более качественные «сложные» модели решающих деревьев можно построить, выбрав критерий ветвления, приводящий к построению дерева принятия решений с наименьшей глубиной так как также снижается сложность рассматриваемого класса решающих функций.

Третья характеристика решающего дерева показывает, на какой глубине больше всего концентрируются листья дерева. Дерево является более сбалансированным, тогда, когда значения глубины дерева и средней глубины листьев дерева достаточно близки друг к другу. Перечисленные характеристики можно использовать и для оценки надежности решающего дерева: чем меньше листьев в дереве, тем выше его надежность.

Определим перечисленные характеристики для деревьев принятия решений, построенных в рамках проводимого исследования, с помощью алгоритмов ID3 и C4.5. Назовем дерево, построенное с помощью алгоритма ID3 первым, а дерево, построенное с помощью алгоритма C4.5 – вторым. Соответственно, характеристики первого дерева будем записывать с верхним индексом 1, а второго – с верхним индексом 2.

$$k^2 = \max_{i=1\ldots\mu^2} k_i^2 = 4; \quad (1)$$

$$k^1 = \max_{i=1\ldots\mu^1} k_i^1 = 5 \quad (2)$$

где k – глубина дерева,

k_i – глубина i-го листа дерева,

1) Вычислим среднюю глубину листьев первого и второго деревьев

$$\Delta k^1 = \sum_{i=1}^{\mu^1} \frac{k_i^1}{\mu^1} \quad (3)$$

$$\Delta k^2 = \sum_{i=1}^{\mu^2} \frac{k_i^2}{\mu^2} \quad (4)$$

где Δk – средняя глубина листьев дерева;

μ – число листьев дерева: $\mu^1 = 33$, $\mu^2 = 26$.

Тогда

$\Delta k^1 = \sum_{i=1}^{\mu^1} \frac{k_i^1}{\mu^1} = \frac{4*5+6*9+8*16}{33} = 4$ – средняя глубина листьев первого дерева

$\Delta k^2 = \sum_{i=1}^{\mu^2} \frac{k_i^2}{\mu^2} = \frac{3*13+2*4+4*8}{26} = 3.03$ – средняя глубина листьев второго дерева.

2) Найдем взвешенную глубину распределения описаний обучающих объектов по листьям дерева.

$$\Delta o^1 = \sum_{i=1}^{\mu^1} \frac{k_i^1 \cdot m_i^1}{m^1} \quad (5)$$

$$\Delta o^2 = \sum_{i=1}^{\mu^2} \frac{k_i^2 \cdot m_i^2}{m^2} \quad (6)$$

где Δo – взвешенная глубина распределения описаний обучающих объектов по листьям дерева,

m_i – число обучающих объектов, описание которых принадлежит интервалу истинности конъюнкции, приписанной листу i;

Тогда

$m^2 = \sum_{i=1}^{\mu^2} m_i^2 = 94;$

$m^1 = \sum_{i=1}^{\mu^1} m_i^1 = 68.$

Тогда

$\Delta o^1 = \sum_{i=1}^{\mu^1} \frac{k_i^1 \cdot m_i^1}{m^1} = \frac{5*68}{68} = 5$ – глубина распределения описаний обучающих объектов по листьям первого дерева.

$\Delta o^2 = \sum_{i=1}^{\mu^2} \frac{k_i^2 \cdot m_i^2}{m^2} = \frac{4*94}{94} = 4$ – глубина распределения описаний обучающих объектов по листьям второго дерева.

3) Обозначим через Δr – «оптимальность» распределения обучающих объектов по листьям дерева:

$\Delta r^1 = \left|\Delta o^1 - \Delta k^1\right| = 5 - 4 = 1$

$$\Delta r^2 = \left|\Delta o^2 - \Delta k^2\right| = 4 - 3.03 = 0.07$$

В таблице 2 представлены все вычисленные характеристики для деревьев принятия решения, построенных с помощью алгоритма ID3 и алгоритма C4.5.

Таблица 2 – Сравнение структурных характеристик решающих деревьев

Алгоритм	μ	k	Δk	Δo	Δr
ID3	33	5	4	5	1
C4.5	26	4	3.03	4	0.07

Из таблицы 2 видно, что дерево, полученное с помощью алгоритма C4.5 имеет более оптимальную структуру.

Оценим качество построенных деревьев с помощью метода LOO («leave-one-out»). Для этого вычислим величину $\tilde{Q}$:

$$\tilde{Q} = \sum_{i=1}^{l} \frac{q_i}{l}, \qquad (7)$$

где q_i – процент правильно классифицированных объектов класса M_i,

l – число классов в обучающей выборке.

В нашей базе данных выходной атрибут имел два возможных значения, поэтому $l = 2$. При построении дерева принятия решений с помощью алгоритма ID3 правильно классифицировались 68 объектов из 99, причем на принадлежность первому классу правильно классифицировались 32 объекта из 45, а на принадлежность второму классу – 36 объектов из 54, то есть

$$\tilde{Q}^1 = \sum_{i=1}^{l} \frac{q^1{}_i}{l} = \frac{(32/45)\cdot 100\% + (36/54)\cdot 100\%}{2} = 68\%$$

При построении дерева принятия решений с помощью алгоритма C4.5 правильно классифицировались 94 объектов из 99, причем на принадлежность первому классу правильно классифицировались 42 объекта из 54, а на принадлежность второму классу – 49 объектов из 54, то есть

$$\tilde{Q}^2 = \sum_{i=1}^{l} \frac{q^2{}_i}{l} = \frac{(42/45)100\% + (49/54)\cdot 100\%}{2} = 86.1\%$$

Результаты приведенных вычислений показывают, что качество построенного дерева выше у алгоритма C4.5.

Таким образом, проведя сравнительный анализ эффективности алгоритмов построения дерева принятия решений для прогнозирования уровня подготовки учителя информатики было выявлено что для построения предсказательных моделей целесообразнее использовать алгоритм C4.5.

В результате исследования был сделан вывод: для того, чтобы уровень подготовки учителя был высоким необходим соответствующий уровень образования. Учитель постоянно находится между практикой и теорией,

наращивая свой опыт преимущественно практическими умениями. Любая педагогическая работа – это практическая деятельность. Часто бывает так, что между теоретическими знаниями и практическими умениями продолжает сохраняться серьёзный разрыв. Преодолеть этот разрыв в современной школе можно средствами профессиональной переподготовки. Повышение квалификации помогает учителю избавиться от устаревших взглядов, делает его более восприимчивым к внешним изменениям, что в конечном итоге повышает его конкурентоспособность [3].

Список литературы

1. Вагин, В. Н. Достоверный и правдоподобный вывод в интеллектуальных системах / В. Н. Вагин., Е. Ю. Головина, А. А. Загорянская, М. В. Фомина // Москва.: ФИЗМАТЛИТ, 2004. – 704 с.

2. Гиглавый, А. В. Долгосрочные тренды развития сектора информационно-коммуникационных технологий / А. В. Гиглавый, А. В. Соколов, Г. И. Абдрахманова, А. А. Чулок, В. В. Буров; Форсайт – FORESIGHT-RUSSIA Т. 7. № 3 – 2013.

3. Симченко, Н. Н. Использование алгоритмов предсказательного моделирования для прогнозирования уровня подготовки учителя информатики [Электронный ресурс] / Н. Н. Симченко // Университетский комплекс как региональный центр образования, науки и культуры : материалы Всерос. науч.-метод. конф, 31 января-02 февраля 2018 г, Оренбург / / Оренбург. гос. ун-т. – Электрон. дан. – Оренбург , 2018. – С. 1859-1865.

МАТЕМАТИЧЕСКОЕ ОБРАЗОВАНИЕ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Смирнова Е.Н.
Оренбургский государственный университет

Математика занимает важное место в науке, культуре и общественной жизни, а также является одной из главных составляющих мирового научно-технического прогресса. В образовании изучение математики играет системообразующую роль: она влияет на преподавание других дисциплин, развивает познавательные способности человека, в том числе логическое мышление. Полноценное математическое образование необходимо каждому человеку для его успешной жизни в современном обществе. Успех нашей страны в XXI веке, эффективность использования природных ресурсов, создание современных технологий, развитие экономики, обороноспособность, зависят от уровня математического образования, математической науки и математической грамотности всего населения страны, от эффективного применения современных математических методов. Без высокого уровня математического образования просто невозможно выполнить поставленную задачу по созданию инновационной экономики, а также реализовать основные цели и задачи социально-экономического развития страны.

Низкая учебная мотивация школьников и студентов связана с непониманием значимости математического образования, перегруженностью образовательных программ общего образования, профессионального образования, а также методических и оценочных материалов устаревшим содержанием и техническими элементами, с отсутствием учебных программ, которые отвечали бы потребностям обучающихся и реальному уровню их подготовки. Все это приводит к несоответствию заданий промежуточной и государственной итоговой аттестации фактическому уровню подготовки большей части обучающихся [1].

На продолжении многих лет математика является важным элементом системы образования всего мира. Это можно объяснить тем, что предмет «Математика» играет значительную роль в формировании личности. Развивающий и образовательный потенциал математики обширен. С помощью математического образования обучающийся познает другие дисциплины. Действие математики сказывается не только в естествознании, но и в социальных и гуманитарных науках. Ссылаются на математические законы и используют математические методы, все отрасли современной науки: физика, химия, биология, медицина, экономика, статистика, лингвистика, социология. Дорога в настоящую жизнь, в современную науку и технику, проходит через математику [5].

Развитие мышления человека в современном мире, реализуемое в ходе общения с другими людьми, в ходе самопознания, а также рассуждений и знакомства с образцами мышления, немыслимо без формирования логической культуры. Строить точный логический анализ ситуаций и выводить следствия из

фактов с помощью логических рассуждений, уметь определять и работать с определениями, отличать неизвестное от известного, недоказанное от доказанного, искусство классифицировать, анализировать, ставить гипотезы, доказывать или опровергать их, использовать аналогии, – все это, а также многое другое, человек изучает в большей мере, конечно, в процессе изучения математики. Математика включает в себя не только формулы и уравнения, но и, правила для точных рассуждений. Учебный предмет математика, содействует воспитанию правильной постановки, лаконичности и строгости речи. Развитие речи обучающихся является главным моментом в формировании культуры мышления [4].

Путь к логике лежит через интуицию. Математическое образование - это способ мышления, формирование привычки находить причины чего-либо, логически мыслить, доказывать всякое утверждение. Если человек не верит недоказанным утверждениям и замечает недостатки в построенных доказательствах, то им невозможно манипулировать. Математика позволяет быстро думать и аргументировать свои результаты, доказывать другим правильность построенной логической цепочки.

Опыт, полученный в ходе выполнения математических задач, позволяет развить такие навыки рационального мышления и способы выражения мысли как ясность, лаконизм, полнота, точность, а также и способность предугадать результат и предвидеть пути решения – интуиции. С помощью математики пробуждается и воображение. Математика – это путь к восприятию научной картины мира, к первым испытаниям научного творчества [2].

Математика вносит значительный вклад не только в общее формирование личности, но и в развитие характера и нравственных черт. Для окончательного решения математической задачи надо проделать очень длинный нелегкий путь. Существуют объективные критерии правильности решения задачи и ее обоснованности, поэтому ошибку невозможно скрыть. Математика способствует формированию настойчивости, способности к работе, интеллектуальной честности, объективности.

Математика развивает эстетическое восприятие мира. Все, кому удалось пережить радостную встречу с блестящей внезапной идеей, решением математической задачи, не станут отрицать, что математика, способна значительно повлиять на эмоциональную сферу человека, включает весомую эстетическую компоненту.

Также курс математики содержит утилитарную, практическую составляющую, имеющую самостоятельное значение. Математика часто встречается и применяется в обыденной жизни. Чтобы ориентироваться в современном мире, каждому просто необходим некоторый набор умений и знаний чисто математического характера, такой как: навыки элементарных вычислений, элементы геометрии – измерение геометрических величин, опознавание и изображение геометрических фигур, умения работать с функцией и ее графиком, составление и решение уравнений, неравенств и их систем, пропорций [3].

Уметь видеть математические закономерности в повседневной жизни и использовать их, на основе математического моделирования, освоение основных математических терминов, символики необходимо в настоящее время каждому образованному человеку. Все это также влияет на развитие личности в современных условиях. Математика требуется для интеллектуального развития личности [6].

Таким образом, математика является как могучим средством решения задач прикладного характера и всеобъемлющим языком науки, так и элементом общей культуры. Математика была и остается главнейшей и существенной компонентой культуры человека, она является необходимым элементом к познанию окружающего нас мира, основой научно-технического прогресса и важной составной частью развития и формирования личности.

Список литературы

1. Концепция развития математического образования в Российской Федерации, утвержденная Постановлением Правительства Российской Федерации № 2506-Р от 24 декабря 2013 года.

2. Гнеденко, Б.В. Математика и математическое образование в современном мире / Б.В. Гнеденко – М.:, Просвещение. – 2005. – 177 с.

3. Кудрявцев, Л.Д. Математическое образование: тенденции и перспективы / Л.Д. Кудрявцев, А.И. Кириллов, М.А. Бурковская, О.В. Зимина // Высшее образование сегодня. − 2002. − № 4. − С. 20–29.

4. Рослова, Л. Влияние современного социума на обучение математике в основной школе / Л. Рослова, С. Суворова, Л. Кузнецова, С. Минаева // Математика. – 2010. – № 14. – С. 3–16.

5. Смирнова Е.Н. Роль математического образования в современном обществе // Международная научно-практическая конференция «Наука – эффективный инструмент познания мира» - г. Новосибирск, 28 августа 2018 г. - 61- 63 с.

6. Фирсов, В.В. О прикладной ориентации курса математики. / В.В. Фирсов // Математика в школе. –2006. – № 6. – С. 2–9.

ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ, ПРЕДСТАВЛЯЮЩИЕ ПРОЦЕСС И РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ СТУДЕНТОМ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ ПО МАТЕМАТИКЕ

Смирнова Е.Н., Томина И.П.
Оренбургский государственный университет

Современный период развития образования характеризуется процессом информатизации, особое значение приобретает применение информационных коммуникационных технологий (ИКТ) в профессиональном образовании. В настоящее время, в соответствии с требованиями ФГОС ВО, к результатам освоения программы бакалавриата по направлению 13.03.02 «Электроэнергетика и электротехника», студенты должны уметь: использовать различные электронные образовательные ресурсы (ЭОР) в учебном процессе и разрабатывать ЭОР для представления результатов учебной, исследовательской деятельности [1]. Однако, как показал анализ исследований, на практике студенты, в основном, лишь заносят информацию в электронном виде о полученных результатах своей деятельности в электронные рабочие тетради или в е-портфолио без представления процесса своей учебной, исследовательской деятельности, а также без анализа и оценивания результатов своей работы. В связи с этим обучение студентов разработке и использованию ЭОР в процессе проведения учебной, исследовательской деятельности является актуальной задачей.

В работе нами разработаны: методические рекомендации по обучению студентов самостоятельной разработке ЭОР; требования к структуре и содержательному наполнению проектных (творческих) ЭОР, под которыми мы понимаем электронные образовательные ресурсы, самостоятельно разрабатываемые студентами для представления процесса и результатов выполненного ими индивидуального (учебного, исследовательского) задания с использованием специализированных программных продуктов, офисных приложений (PowerPoint, Excel, Word) и распределенных информационных ресурсов.

Требования к структуре и содержательному наполнению проектных (творческих) ЭОР.

Нами предложено выделить в структуре проектного (творческого) ЭОР следующие разделы: главное окно (страница); формулировка индивидуального задания для проведения учебной, исследовательской деятельности; обоснование цели и задач индивидуального задания; предъявление процесса выполнения индивидуального задания; представление результатов индивидуального задания. Охарактеризуем кратко каждый раздел проектного (творческого) ЭОР.

Главное окно ЭОР – это своеобразный титульный лист, на котором представлены: название темы индивидуального задания; фамилия, имя, отчество студента; группа в которой он учится; фамилия, имя, отчество руководителя (преподавателя) индивидуального задания.

Формулировка индивидуального задания. В этом разделе студенты должны сформулировать актуальность своей работы, обосновать, где будут использованы полученные результаты, представить исходные данные индивидуального задания.

Выполнение индивидуального задания. Данный раздел ориентирован на представление процесса выполнения индивидуального задания с наглядно-образным пояснением каждого выполненного действия (текст, график, диаграмма).

Представление результатов индивидуального задания. В данном разделе проектного (творческого) ЭОР обучающийся представляет результаты выполненного задания и проводит их анализ.

Разработанный студентом проектный (творческий) ЭОР предлагается рассматривать как самостоятельный тип ЭОР, который в процессе обучения может быть архивирован либо на платформе Moodle, либо на личной страничке обучающегося, размещенной в «облаке», либо аккумулирован в блок индивидуальных заданий е-портфолио [2].

К содержательному наполнению проектных (творческих) ЭОР в работе обоснованы и сформулированы требования:

– логичности – строгая логическая последовательность выполненных обучающимся математических действий с использованием редактора формул, специализированных программных продуктов;

– пошагово-подробное представление математических действий – пояснение каждого выполненного действия с применением текстового, графического редакторов, офисных приложений;

– демонстрация результатов – наглядно-образное представление полученных результатов в виде презентации выполненного индивидуального задания.

Заполнение разделов проектных (творческих) ЭОР в соответствии с предлагаемыми требованиями к содержательному наполнению способствует формированию у студента «следов памяти», которые позволяют быстро вспомнить и воспроизвести раннее изученный материал, необходимый при изучении последующих дисциплин, а также при выполнении курсовых работ и проектов.

Фрагменты раздела «Выполнение индивидуального задания» проектных (творческих) ЭОР, разработанных студентами Оренбургского государственного университета, представлены на рисунке 1.

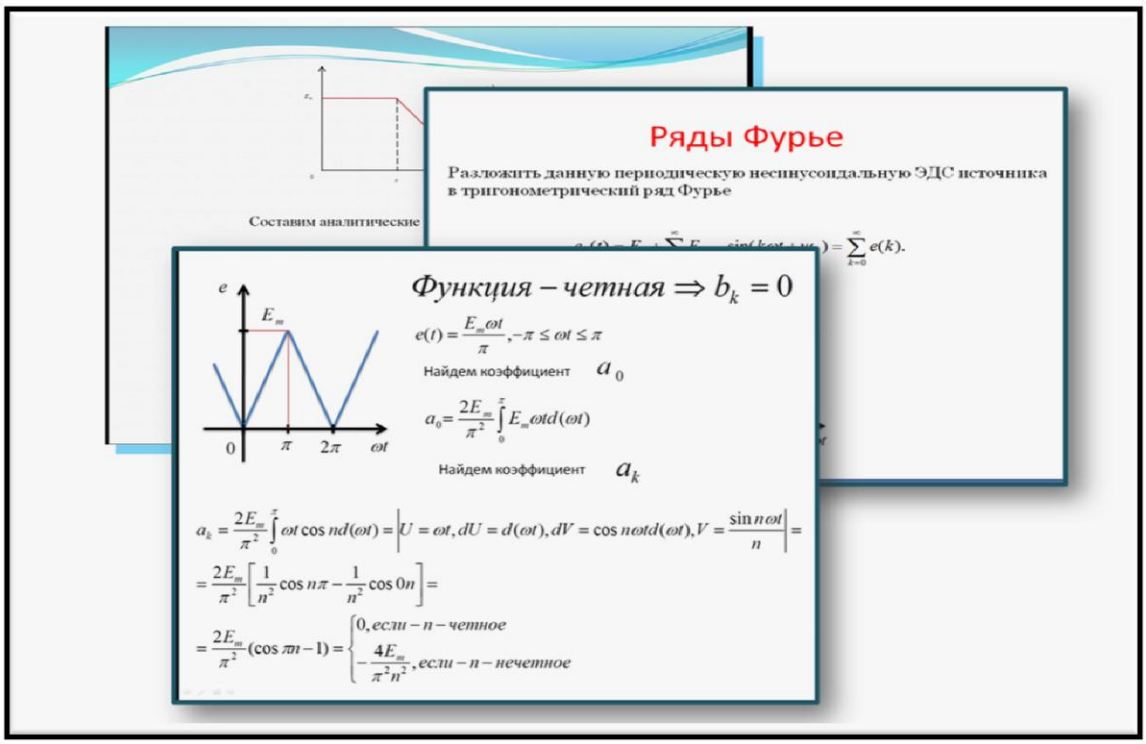


Рисунок 1 - Скриншоты проектных (творческих) ЭОР

Опираясь на работы Мухаметзянова И.Ш., Мартиросян Л.П., Роберт И.В., Димовой А.Л., нами обоснованы и сформулированы следующие эргономические требования к разработке проектного (творческого) ЭОР: фигуро-фонового соотношения (цветовой гармонии); требования к шрифтам, символам, формулам; организации информации внутри окна; требования при работе с несколькими окнами; организация аудиоинформации; требования к анимированным изображениям. Содержательная характеристика каждого требования подробно изложена в работе [3]. Комфортно организованная визуальная среда с учетом индивидуальных особенностей обучающихся, позволяет облегчить процесс восприятия учебного материала и исключает утомление при работе.

Методические рекомендации.

Обоснованы и разработаны методические рекомендации по разработке студентами проектных (творческих) ЭОР, ориентированных на: выполнение эргономических требований и требований к структуре и содержательному наполнению ЭОР; реализацию дидактических возможностей ИКТ: интерактивный диалог; компьютерная визуализация учебной информации; компьютерное моделирование; архивирование; автоматизация процессов вычислительной, информационно-поисковой деятельности, распространения учебной информации [4]. Методические рекомендации по разработке студентами проектных (творческих) ЭОР были внедрены и использованы в учебном процессе ФГБОУ ВО «Оренбургский государственный университет» на электроэнергетическом факультете при обучении математике, в течении пяти лет.

Получены следующие результаты: 79,2% студентов достигли эвристического и творческого уровней обученности в области разработки проектных (творческих) электронных образовательных ресурсов, в процессе обучения, основанном на реализации разработанных авторами методических рекомендаций. Полученный результат свидетельствует о выполнении поставленной задачи.

Список литературы

1. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 13.03.02 «Электроэнергетика и электротехника», утвержденный приказом Министерства образования и науки РФ от 03.09.2015, № 955.

2. Семенова, Н. Г. Структура электронного портфолио для студентов технических специальностей / Н. Г. Семенова, И. П. Томина // Информационная среда образования и науки. – 2011. – № 4. – С. 113-116.

3. Семенова, Н. Г. Психолого-педагогические требования к мультимедийным обучающим системам технических дисциплин: монография / Н. Г. Семенова. – Оренбург : ГОУ ОГУ, 2006. – 145 с.

4. Роберт, И.В. Теория и методика информатизации образования (психолого-педагогический и технологический аспекты) / И.В. Роберт. / М.: БИНОМ: Лаборатория знаний, 2014.

ДИДАКТИЧЕСКИЕ ОСНОВЫ ПРИМЕНЕНИЯ ОБУЧАЮЩЕЙ СРЕДЫ MOODLE ПРИ ИЗУЧЕНИИ МАТЕМАТИКИ В УНИВЕРСИТЕТЕ

Тарасова Т.Н. канд. пед. наук, доцент, Руцкова И.Г.
Оренбургский государственный университет

Объективно существующие противоречия между необходимостью изучения больших объемов теоретического учебного материала, отработки его практических приложений и формирование навыков их использования в короткие сроки требуют интенсификации образовательного процесса.

К проблемам оптимизации и интенсификации в дидактике высшей школы советские и российские исследователи обращаются начиная с фундаментальных работ Ю.К. Бабанского, В.П. Беспалько, В.В. Давыдова, С.И. Архангельского и др. отечественных ученых. Детально разработаны в педагогике и подходы к структурированию содержания образования (В.С. Леднев, Г.Н. Серинов, М.Н. Скаткин и др.). Одним из инновационных направлений интенсификации образовательного процесса является использование модульно-рейтинговой технологии, основанной на синтезе технологий модульного обучения и рейтинговой системы контроля и оценки знаний. Основателями модульно-рейтинговой технологии являются С. Постлешвайт, Дж. Рассел, Р. Хорст. П.А. Юцявичене, М.А. Чошанов. Повышение эффективности обучения в современных условиях связано, прежде всего, с рациональным использованием дидактических возможностей информационных технологий в высшей школе, направлением, активно развивающимся начиная с исследований Л.Х. Зайнутдиновой, В.А. Красильниковой, Е.С. Полат, И.В. Роберт и др.

Анализ теоретических положений и многолетний педагогический опыт практического применения различных подходов к оптимизации процесса математической подготовки студентов в условиях университета, позволяет нам, в настоящих условиях, в качестве перспективного направления назвать синтез идей модульного обучения, основанной на них модульно-рейтинговой технологии и их компьютерной реализации [1, 2].

Достоинства модульного подхода в обучении достаточно детально изучены современной дидактикой высшей школы. Среди них: широкие возможности удовлетворения индивидуальных потребностей обучающегося в создании и реализации индивидуальных образовательных маршрутов; возможность интегрировать информацию по различным основаниям: базовые знания, профессионально ориентированные, обладающие исследовательским потенциалом и т.п.; организация субъект - субъектного взаимодействия с акцентом на деятельность обучающегося и т. д.

Вместе с тем, появляются исследования, посвященные непосредственно реализации модульного обучения с использованием информационных технологий. Так, Е.И. Ряполова, выделила некоторые принципы компьютерной реализации модульного обучения:

- компактность модульной программы - возможность ее установки и использования на различных устройствах, в различных территориальных и временных условиях;

- цикличность, позволяющая обучаемому несколько раз проходить по циклу обучения;

-практическая направленность, отражающая взаимосвязь теории с практикой;

-логическая преемственность, реализующая, в том числе, и уровневую дифференциацию;

- логическая завершенность, обеспечивающая включение в модуль всю информацию, необходимую для изучения, закрепления и проверки знаний и др. [3].

Модульно-рейтинговая технология представляет собой образовательную технологию, в которой в качестве цели обучения выступает совокупность компетенций обучающихся, в качестве средства ее достижения - создание соответствующих педагогических условий. В образовательной практике именно рейтинговая оценка знаний и умений обучающихся чаще всего используется при модульном обучении, поскольку рейтинговая система нацелена, прежде всего, на повышение мотивации студентов к освоению содержания образования на основе дифференциации оценки их учебной работы. Рейтинговая оценка обученности студента позволяет с большой степенью доверительности характеризовать качество его подготовки. Далеко не каждая рейтинговая система обеспечивает качественную оценку - выбранная произвольно, без доказательств ее эффективности и целесообразности, она может стать формальным показателем, не отражающим объективный результат. Проблема заключается в том, что разработать критерии знаний и умений, а также их оценки - дело очень трудоемкое [4].

Обращаясь к информационно-технологическим аспектам реализации модульно-рейтинговой технологии, можно констатировать наличие на современном рынке программного обеспечения достаточно широкого спектра программных продуктов, в том числе и платформ для создания электронных образовательных ресурсов, предполагающих различные практики внедрения информационных технологий в образовательный процесс. Одной из таких образовательных платформ является обучающая среда Moodle. Эта модульная объектно-ориентированная динамическая среда является одной из наиболее часто используемых для организации учебного процесса в русскоговорящем сегменте Интернета. Широкая популярность продукта основывается на ее доступности (является полностью бесплатной) и завершенности (представляет собой готовое коробочное решение).

Платформа обладает широкими возможностями, основными из которых являются: учет обучаемых, возможность их идентификации и разграничения прав доступа к материалам; ведение отчетности и статистики по обучению; контроль и оценка уровня знаний; использование текстовых, графических, аудио и прочих материалов внутри системы; анкетирование, создание

опросов и многие другие. К очевидным достоинствам платформы Moodle необходимо отнести: доступность, простоту использования, высокую производительность, возможность ее адаптации под конкретные задачи и т.д.

Рассматривая платформу Moodle как средство компьютерной реализации модульно-рейтинговой технологии, необходимо отметить, что она представляет собой проработанную реализацию учебного процесса, основанного на принципах модульного обучения и рейтингового контроля знаний обучающихся.

Старшим преподавателем кафедры прикладной математики ОГУ И.Г. Руцковой, в рамках разработки одного из направлений ГБ НИР «Информационно-математическое обеспечение реализации системного подхода в исследованиях проблем образования» (№ госрегистрации 01201252685), на протяжении ряда лет осуществляется реализация учебных программ математических дисциплин на различных специальностях и направлениях бакалавриата на основе рассмотренных дидактических принципов. Опубликован ряд работ, содержащих промежуточные результаты и анализ возможностей использования платформы Moodle в организации учебного процесса [1, 2, 5, 6, 7].

Полученные результаты подтверждают, что реализация модульно-рейтинговой технологии в обучающей среде Moodle в значительной мере повышает эффективность и качество математической подготовки студентов бакалавриата, прежде всего за счет интенсификации информационно-деятельного процесса обучения и использования дифференцированной системы контроля.

Список литературы

1. Руцкова, И.Г. Использование возможностей электронной системы обучения Moodle при реализации балльно-рейтинговой системы оценки освоения математических дисциплин /И.Г. Руцкова //Университетский комплекс как региональный центр образования, науки и культуры. Материалы Всероссийской научно-методической конференции; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Оренбургский государственный университет" – Оренбург: ООО «ИПК университет», 2014. С. 2902-2909. ISBN: 978-5-4417-0309-3.

2. Руцкова, И.Г. Анализ эффективности использования электронной системы обучения Moodle в процессе преподавания математических дисциплин /И.Г. Руцкова //Сборник материалов Международной научной конференции: «Наука и образование: фундаментальные основы, технологии, инновации», посвященной 60-летию Оренбургского государственного университета. – Оренбург: ОО ИПК «Университет», 2015. ISBN 978-5-4417-0557-8 Часть 4 – С. 27 – 31. ISBN 978-5-4417-0561-5.

3. Ряполова, Е.И. Проблема компьютерной реализации модульного обучения студентов через призму компетентностного подхода/Е.И. Ряполова//

Реализация компетентностного подхода в сфере инженерной подготовки: авторская монография. – Уфа: АЭТЕРНА, 2017. - С. 125-134. ISBN 978-5-00109-346-6.

4. Бережная, И.Ф. Активизация процесса обучения курсантов в военно-учебных заведениях на основе применения модульно-рейтинговой технологии /И.Ф. Бережная, А.В. Столяров // Перспективы науки. - 2011. № 2 (17) С.16 - 19.

5. Руцкова, И.Г. Использование возможностей электронной системы обучения Moodle в процессе организации и контроля самостоятельной работы студентов при изучении математических дисциплин / И.Г. Руцкова // Математика. Информационные технологии. Образование [электронный ресурс]: материалы III Всероссийской научно-практической конференции, Оренбург, 8-9 декабря 2011 г. – Электрон. данные. – Оренбург: Руссервис, 2011./Секция 4. Информационно-математическое обеспечение организации и мониторинга качества образовательных процессов. - Оренбург, ОГУ – 2011. - ISBN 978-5-904627-21-8.

6. Руцкова И.Г. Методическая поддержка и контроль самостоятельной работы студентов по математике средствами Moodle / И.Г. Руцкова // Рожественские чтения: тезисы докладов XVI Межрегиональной научно-методической конференции по вопросам применения ИКТ в образовании 9 января 2012 года. - Пермь: Перм. гос. Нац. Иссл. Ун-т, 2012. – Вып. 16. – С. 103 – 106.- ISBN 978-5-7944-1599-5

7. Руцкова, И.Г. Электронный учебно-методический комплекс «Теория вероятностей и математическая статистика» в системе электронного обучения Moodle как средство методической поддержки, организации и контроля самостоятельной работы студентов /И.Г.Руцкова //Университетский комплекс как региональный центр образования, науки и культуры. Материалы Всероссийской научно-методической конференции; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Оренбургский государственный университет" – Оренбург: ООО «ИПК университет», 2014. С. 3075-3081. ISBN: 978-5-4417-0309-3.

ИНТЕРНЕТ-СЕРВИСЫ КАК СРЕДСТВО РАЗРАБОТКИ КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫХ ЗАДАНИЙ

Токарева М.А., канд.техн.наук, доцент, Кулантаева И.А., канд.пед.наук
Оренбургский государственный университет

Развитие процессов информатизации существенно влияет на характер социальных требований к системе образования. Современная парадигма компетентностно-ориентированного обучения направлена на комплексное освоение знаний и способов практической деятельности, обеспечивающих успешное функционирование человека в ключевых сферах жизнедеятельности в интересах как его самого, так и общества в целом.

Приобретаемое при этом знание характеризуется не столько количеством известных фактов, сколько умением применять их в профессиональной области, в смежных областях, а порой и в ситуациях, в которых явно не прослеживается связь возникшей проблемы и предметного знания. Поэтому современный образовательный процесс должен заключаться не просто в передаче обучающимся предметных знаний, которые имеют отдаленную перспективу их использования, а в демонстрации применения этого знания для решения актуальных профессиональных и квазипрофессиональных проблем, а также создания условий для самостоятельного решения обучающихся таких проблем в учебном процессе.

Внедрение компетентностно-ориентированных заданий в предметное обучение – одно из направлений, связанных с реализацией действующих стандартов в образовании. Компетентность при выполнении таких заданий не противопоставляется знаниям или умениям, она включает их в себя, но не путём простого суммирования, а при свободном использовании наиболее эффективного для конкретной ситуации набора из имеющихся в арсенале обучающегося знаний и умений.

Компетентностно-ориентированные задания выполняют не столько контролирующую, сколько формирующую функцию. Действительно, в соответствии с основными положениями психологии и педагогики задания, моделирующие некоторую деятельность, требуют для выполнения этой деятельности актуализации определенных знаний, умений, способностей, личностных качеств, компетентностей. И в процессе этой актуализации данные категории не только проявляются, но и потенциально развиваются. Многие из таких заданий предполагают самостоятельный поиск информации: человек должен оценить, насколько имеющаяся у него информация неполна, и уметь «добрать» ее. Это одна из общих компетенций: уметь понять, чего тебе не хватает для решения поставленной задачи, найти, использовать какие-то дополнительные материалы.

Компетентностно-ориентированные задания сохраняют учебное занятие как одну из форм организации обучения, но упор делается на расширение

применения иных форм организации занятий, такие как сессия, групповая работа над проектом, самостоятельная работа в библиотеке и за компьютером и прочее.

В рамках руководства прохождением производственной педагогической практики студентами направления 44.03.01 Педагогическое образование, профиль «Информатика», нами был разработан комплект компетентностно-ориентированных заданий по информатике для 8 класса с целью апробации методики их создания с использованием современных интернет-сервисов. На примере разработанного комплекта заданий демонстрируется возможности организации контроля усвоения материала учащимися при изучении дисциплины «Теория и методика обучения информатике» для бакалавров указанного направления.

Компетентностно-ориентированные задания по информатике выполняют следующие функции:

- мотивационную (представление жизненной (проблемной) ситуации с привлечением актуального для ученика материала обеспечивает его внутреннюю мотивацию);
- создание психологически комфортных условий для организации и осуществления учебной деятельности;
- активизации познавательной деятельности (внутреннее побуждение мобилизует школьника, активизирует его мыслительную деятельность);
- организационную (наличие плана действий помогает ученику выстроить правильный маршрут следования и решения поставленных задач);
- формовочную (усваиваются способы действий, вырабатываются умения не только оперировать предметным материалом, но и привлекать знания и умения из смежных дисциплин, обще- учебные знания и умения);
- оценочную (поскольку компетентность проявляется лишь в деятельности, именно применение компетентностно ориентированных вопросов, задач и тестов позволяет выявить уровень её сформированности);
- мировоззренческую (ученик получает возможность увидеть целостную картину мира во взаимосвязи и взаимозависимости фактов и явлений из разных сфер, учебных предметов и т. п.);
- личностную (через создание ситуации успеха способствует утверждению личностью собственного «Я») [1].

Одним из приоритетных средств реализации компетентностного подхода в образовании является использование компетентностно-ориентированных заданий. В настоящий момент разработана их структура, описаны специфические особенности, но дидактические материалы с готовыми к внедрению в процесс обучения компетентностно-ориентированными заданиями отсутствуют. Имеющиеся в литературе компетентностно-ориентированные задания приводятся в качестве примеров, иллюстраций основных положений компетентностного подхода. Поэтому практикующие учителя вынуждены самостоятельно разрабатывать специальные задания для формирования и оценивания компетентностей по своей дисциплине или на межпредметном содержании. Способность сконструировать компетентностно-ориентированные

задания в свою очередь позволяет оценить и профессиональную компетентность самого преподавателя. В зависимости от содержания дисциплины и особенностей развиваемых компетентностей конструирование соответствующего компетентностно-ориентированного задания может приобретать некоторую специфичность. Тем не менее, анализируя собственный опыт составления компетентностно-ориентированного задания и опыт коллег, на наш взгляд, можно говорить об обобщенном алгоритме конструирования таких заданий. Выделим его основные составляющие:

- определение аспекта(-ов) компетентности, подлежащего(-их) формированию или оценке;
- составление задачи на основе выбранного аспекта;
- поиск источников, позволяющих реализовать планируемую деятельность;
- формирование мотивов и стимулов;
- создание ключей или модельных ответов, шкал, бланков и инструкций к предъявлению результата решения задачи;
- самоэкспертиза задания.

Приведенный эмпирический алгоритм отражает основные структурные компоненты компетентностно-ориентированного задания, но последовательность их конструирования отлична от последовательности их предъявления в готовом задании. Ориентированность компетентностных заданий на создание ими условий для овладения методами приобретения знаний обучающимися свидетельствует о формировании методологической культуры как части исследовательской культуры школьника. Компетентностно-ориентированные задания могут быть сконструированы и представлены для использования в практике обучения в различных модификациях. Современной дидактике известны такие их формы, как:

- обобщенная компетентностная задача;
- задача-аналогия;
- задача-модель;
- задача-поиск прообраза;
- задача-структурирование; задача-возможность;
- задача на избыточность, задача на недостаточность.

По характеру учебно-познавательной деятельности:

- обучающие, поисковые, проблемные;
- по содержанию – предметная, межпредметная, практическая задачи;
- по преобладающему компоненту деятельности;
- теоретической или практической направленности.

Заметим, что особое место в достижении планируемых результатов образования следует отвести ситуационным и практическим задачам. Авторским коллективом РГПУ им. А.И. Герцена разработана структурная модель ситуационных задач:

- название задания;

- личностно-значимый познавательный вопрос;
- информация по данному, вопросу, представленная в разнообразном виде (текст, таблица, график, статистические данные и т. д.);
- задания на работу с данной информацией.

При сравнении со структурой компетентностно-ориентированного задания легко находим уже известные компоненты: первый – второй соответствуют стимулу; третий компонент ситуационной задачи представляет собой источник информации, а четвертый – задачную формулировку [2].

Для эффективной работы в современных условиях развития образования необходимо использовать технологии, которые позволяют быстрее и удобнее работать с информацией, планировать свою работу, поддерживать коммуникацию, расширять возможности учебной и исследовательской деятельности. Поэтому для создания компетентностно-ориентированных заданий по информатике мы обратились к готовому инструментарию, предоставляемому современными интернет-сервисами.

Интернет-сервисы – это сайты, представляющие в основном бесплатные услуги для аудитории Интернета. Наиболее распространенными интернет-сервисами являются:

- хранение данных;
- передача сообщений и блоков данных;
- электронная и речевая почта;

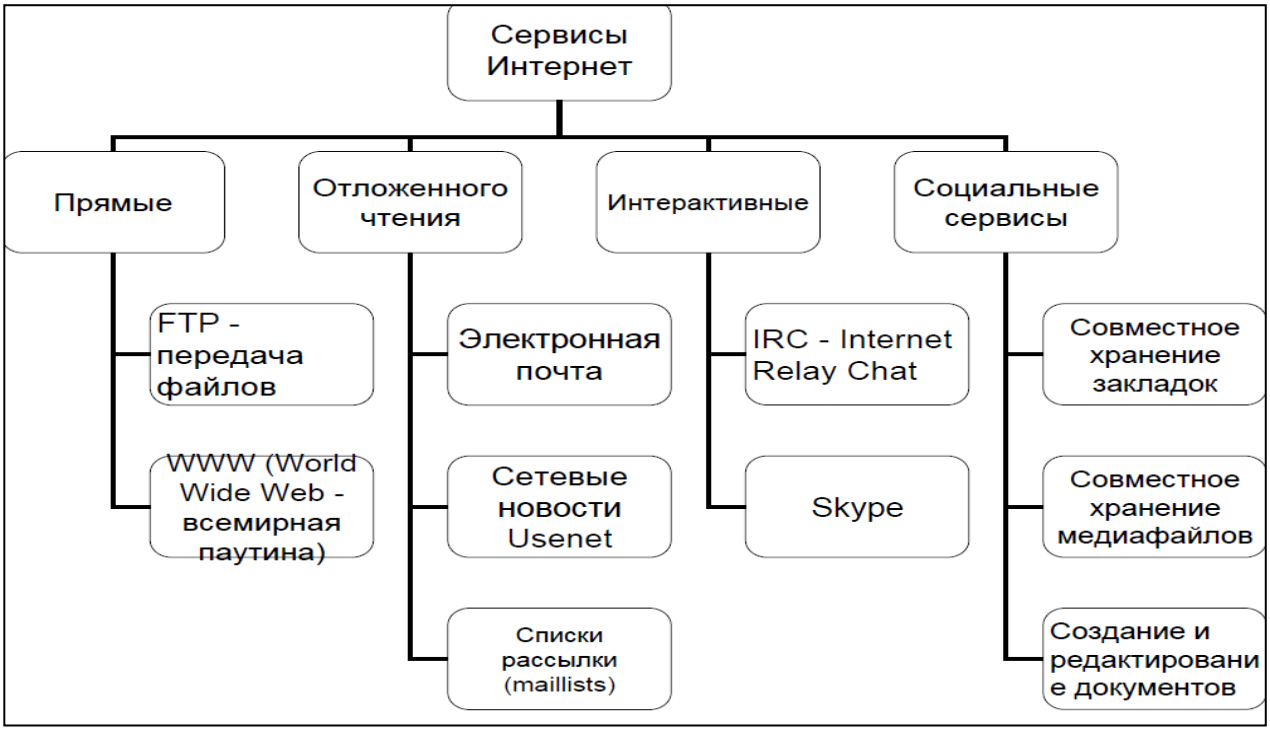


Рисунок 1 – Классификация интернет-сервисов

- организация и управление диалогом партнеров;
- предоставление соединений;
- проведение сеансов;

- видео-сервис и т.д.

Классификация интернет-сервисов представлена на рисунке 1.

Нами была проанализирована учебно-методическая и справочная литература по вопросам создания компетентностно-ориентированных заданий в интернет-сервисах uCoz, Wix, Nethouse, Сайты Google. Критериями выбора стали: платформа, адаптивность, шаблонов, возможность создать сайт с нуля, обучающие материалы, возможность редактировать и добавлять код, уровень пользователей, бесплатный тариф.

Исходя из анализа современных интернет-сервисов были выбраны сервисы Google, LearningApps, Draw.io, так как они наиболее удобные для реализации компетентностно-ориентированных заданий.

Для размещения в сети необходимо выбрать платформу, на которой будут размещены задания. С помощью таблицы 1 мы проанализировали, какая платформа наиболее подходит для размещения заданий.

Использовалась трех-бальная шкала, где 3 означает «есть», 2 - «частично», 1 – «отсутствует».

Таблица 3 – Анализ выбора платформы

Платформа	uCoz	Wix	Сайты Google	Nethouse
Адаптивность шаблонов	3	3	3	2
Возможность создать сайт с нуля	3	3	3	3
Обучающие материалы	2	3	3	1
Возможность редактировать и добавлять код	3	2	3	2
Уровень пользователей	1	1	3	3
Бесплатный тариф	2	2	3	3

После проведенного анализа мы выбрали платформу сайтов Google, так как она соответствует выбранным нами критериям (Рисунок 2).

При конструировании набора компетентностно-ориентированных заданий мы опирались на известную, разработанную американским ученым Б. Блумом, классификацию результатов обучения. Таксономия Б. Блума охватывает три сферы: когнитивную (познавательную), эмоциональную и психомоторную, каждая из которых характеризуется восходящим порядком сложности. Ученым была предложена шестиуровневая иерархическая структура когнитивной (познавательной) сферы.

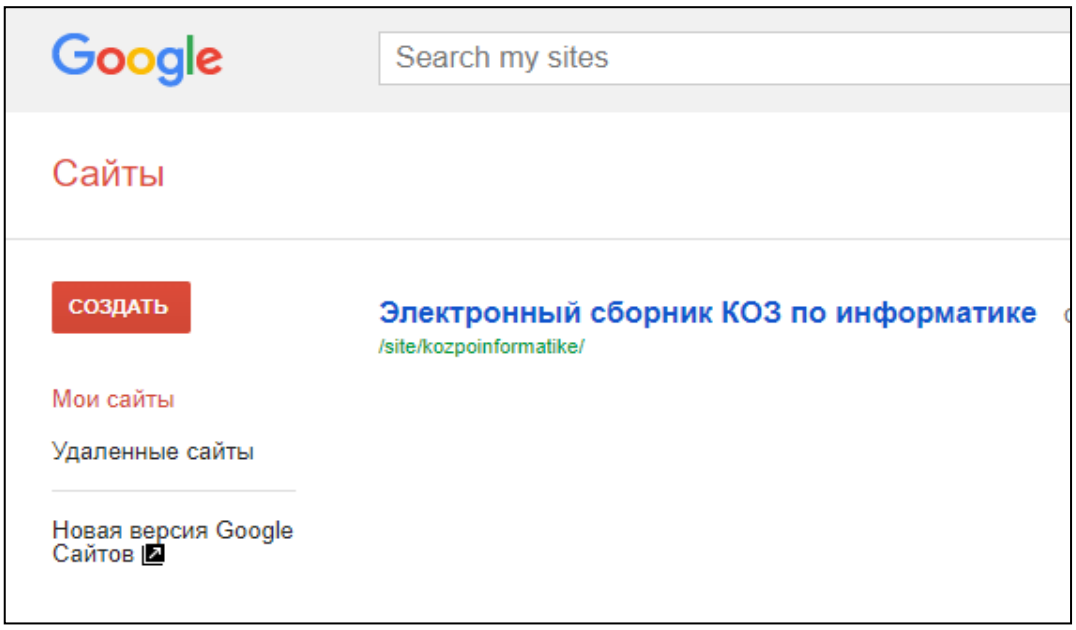


Рисунок 2 - Создание сайта на платформе сайтов Google

Содержательная составляющая разработки компетентностно-ориентированных заданий опирается на проведенный нами анализ двух учебно-методических комплексов авторов Л.Л. Босовой и Н.Д. Угринович, составленных согласно действующему федеральному государственному образовательному стандарту.

При рассмотрении разделов и входящих в них тем, в общей сложности с помощью интернет-сервисов было разработано 10 компетентностно-ориентированных заданий по следующей тематике:

- Системы счисления.
- Элементы алгебры логики.
- Основные алгоритмы конструкции.
- Организация ввода и вывода данных.
- Программирование линейных, разветвляющийся и циклических алгоритмов.
- Построение диаграмм и графиков в электронных таблицах.
- Кодирование и обработка числовой информации.
- Кодирование текстовой информации.
- Базы данных в электронных таблицах.
- Сортировка и поиск данных в электронных таблицах.

Структуру сборника определяют:

1) Блок заданий.
2) Общие рекомендации.
3) Блок обратной связи.
4) Блок дополнительных материалов.

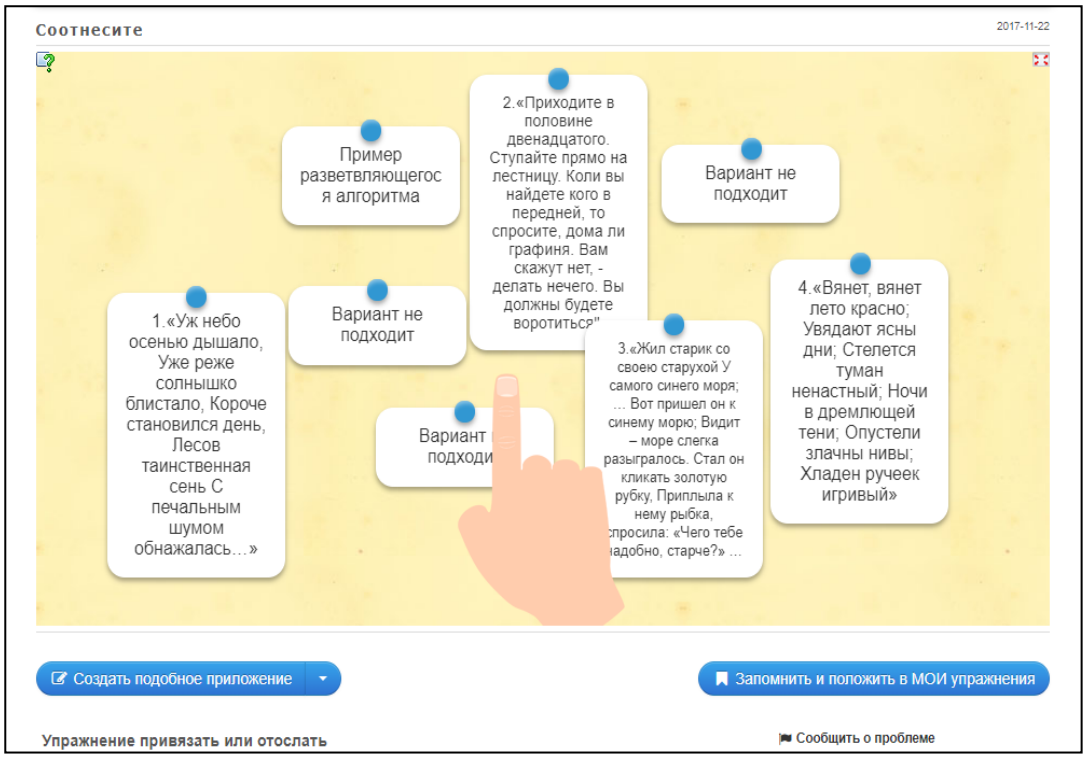


Рисунок 3– Фрагмент задания с использованием LearningApps

Время на выполнение задания – 15 минут согласно документу «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных организациях» (СанПиН 2.4.2.2821-10).

Примеры разработанных компетентностно-ориентированных заданий приведены на рисунках 3, 4.

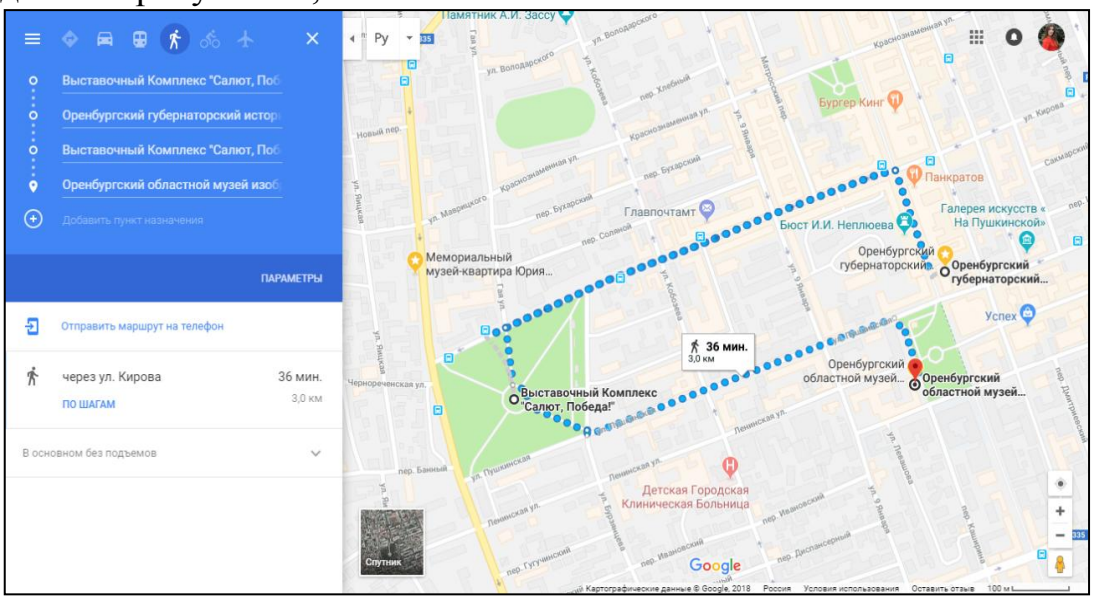


Рисунок 4 – Фрагмент задания с использованием интернет-сервиса Google-карты

Работая со сборником, пользователь может с помощью панели навигации по элементам перейти на предыдущий или следующий элемент, или выбрать нужный элемент сборника.

Элементы сборника – это созданные страницы сайта, с помощью которых учитель организует учебный процесс (размещает материалы заданий, общается с учениками). Платформа располагает большим разнообразием сервисов, которые могут быть использованы для размещения заданий любого типа.

Сборник компетентностно-ориентированных заданий предназначен для обогащения учебно-методического обеспечения образовательного процесса по дисциплине «Теория и методика обучения информатике», был успешно апробирован в Муниципальном общеобразовательном бюджетном учреждении «Средняя образовательная школа № 34» города Оренбурга.

По результатам апробации можно заключить, что использование компетентностно-ориентированных заданий позволяет развивать у обучающихся критическое мышление, творческие способности, коммуникативные умения и навыки, устанавливать эмоциональные контакты между учащимися. Это способствует повышению мотивации к изучению информатики, помогает в решении воспитательных задач.

Список литературы

1 Ефремова, Н. Ф. Компетенции в образовании. Формирование и оценивание / Н. Ф. Ефремова. – М.: Национальное образование, 2015. – 416 с.

2 Абдуразаков, М. М. Направления совершенствования подготовки к профессиональной деятельности будущего учителя информатики / М. М. Абдуразаков, Г. М. Гаджиев // Информатика и образование. – 2006. – № 2. – С. 98-102.

МОДЕЛЬ РАСПРЕДЕЛЕННОЙ ГЕТЕРОГЕННОЙ МУЛЬТИОБЛАЧНОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ И ПЛАТФОРМЫ АВТОМАТИЗАЦИИ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ ДЛЯ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Ушаков Ю.А., канд. техн. наук, доцент,
Бахарева Н.Ф., д-р техн. наук, профессор,
Полежаев П.Н., Шухман А.Е., канд. пед. наук, доцент
Оренбургский государственный университет

В данной работе будет рассматриваться структурная модель современного центра обработки данных (ЦОД), построенного по иерархической модели, с учетом последних тенденций по построению таких сетей: сети без границ (Borderless), применение VXLAN, виртуализация сетевого оборудования, программное управление хранилищами и сетями.

Поскольку с внедрением виртуализации повсеместно стали виртуализироваться маршрутизаторы, брандмауэры, шлюзы VPN, коммутаторы, то в работе для всех описываемых узловых элементов будет введена ссылка на родительский граф/узел для возможности описания вложенных систем (например, шлюз в контейнере в виртуальной машине на сервере). Для сетевой связности информация о вложенности требуется для описания каналов связи по причине того, что множество соединений с виртуальными устройствами будет проходить через одно и то же физическое подключение со своими ограничениями, в то же время для коммутации и маршрутизации информация о вложенности не требуется.

Для каждого элемента структурной модели будет использован уникальный однобуквенный индекс $[1..\max(кол.элементов)]$, для краткости введем обозначение $m(индекс)$ – максимальное значение.

- s – индекс сегмента *Segment;*
- *p* – индекс провайдера *ISP*;
- k – индекс сетевого узла любого типа *Node, Switch, Storage;*
- d – индекс ЦОД *Datacenter;*
- e – индекс сетевого интерфейса *p*;
- l – индекс связи *Links, ExtLinks*.

Для упрощения описания вложенных элементов будем использовать объектный метод представления структуры через указатель на родительский элемент, например $Datacenter_d \to Segment_s \to Node_k \to Container_c \to p_e$, для краткости может использоваться верхний набор индексов в порядке иерархии вложенности, например, $p_e^{(d,s,k,c)}$ означает, что сетевой интерфейс расположен в контейнере *c*, который расположен в узле *i*, который расположен в сегменте *k*, который находится в ЦОД *s*. Каждый индекс в схеме является глобальным и может быть использован, как глобальный индекс множества для прямого доступа к элементу.

Для схемы всей сети будут верными следующие утверждения:

- вся схема, относящаяся к сетевой инфраструктуре будет разбита по уровням OSI: 1 (физический), 2 (канальный), 3 (сетевой), 4 (транспортный) и 7 (приложения). Это позволит согласовать видение сети с традиционными схемами и более гибко подходить к описанию сложных структур;
- каждое сетевое устройство будет представлено как элемент *Node*, для дополнительного описания которого используются отдельные расширяемые классы устройств (например, *Storage* для описания особенностей сетевых хранилищ или *Switch* для описания коммутатора);
- каждое сетевое устройство имеет хотя бы один сетевой интерфейс физического уровня, в том числе виртуальные и подинтерфейсы *p*;
- каждый сетевой интерфейс должен быть соединен с другим сетевым интерфейсом через канал связи *Link*, иначе он считается отключенным;
- виртуальные каналы связи *VirtualLink* также должны начинаться и заканчиваться в сетевых интерфейсах, но могут иметь дополнительную привязку по 2 и 3 уровням интерфейсов;
- путь *Path* – это набор пар интерфейсов, опционально дополненных интерфейсами верхних уровней, вплоть до 4 (транспортного) – для потока приложения, балансировщиков, прокси.

Пример описания взаимосвязи и зависимости элементов сети показан на рисунке 1.

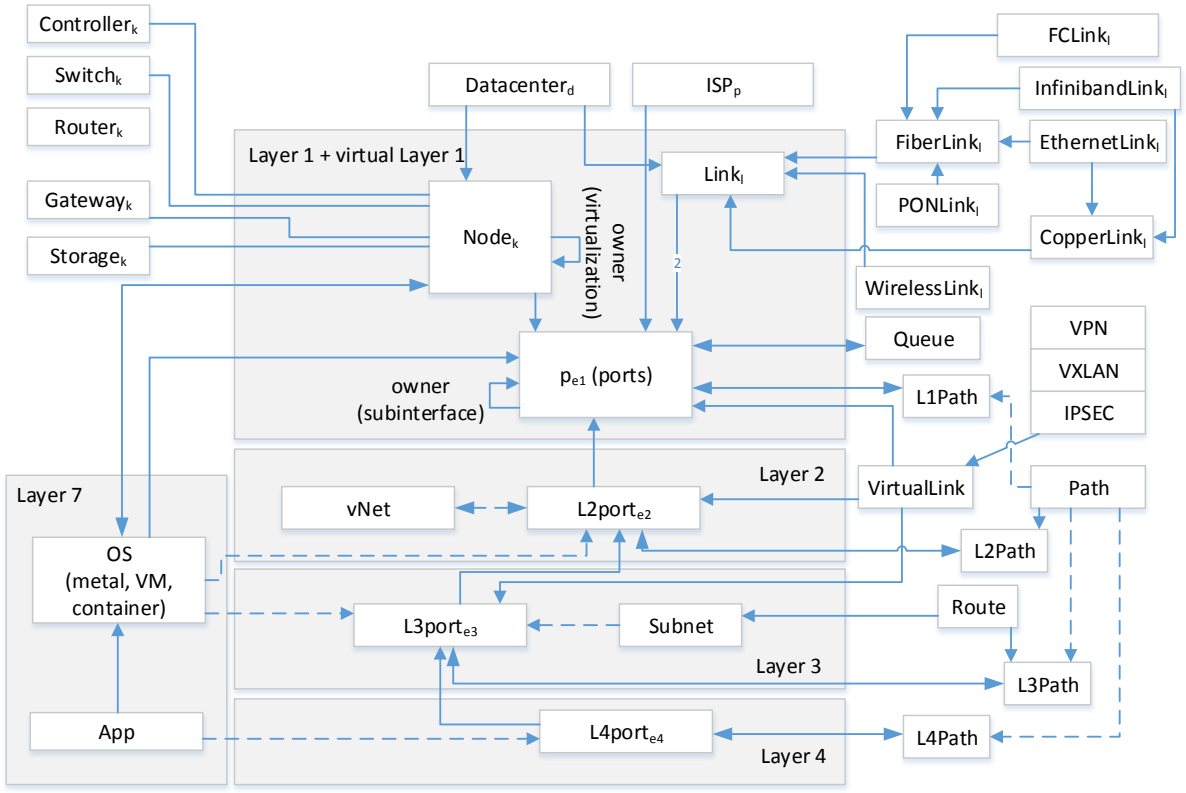


Рисунок 1 – Структура и взаимоотношения элементов схемы

Структура распределенной мультиоблачной системы может быть определена в виде ориентированного мультиграфа вида:

$$MultiCloud = (\{Datacenters, ISP\}, WANLinks), \quad (1)$$

где вершины $Datacenters = \{Datacenter_1, Datacenter_2, ..., Datacenter_\varsigma\}$ – множество отдельных территориально разделенных облачных сегментов (автономных систем, ЦОД), связанных между собой через глобальные сети;

$WANLinks(t) = \{Link_l \cup VirtualLink_l\}$ – дуги, представляющие направленные связи (VPN каналы) между сегментами через глобальные сети, $Link_i = (p_i, p_j)$, где p_i, p_j - порты устройств, осуществляющих соединение между разными ЦОД и провайдерами или напрямую между разными ЦОД виртуальным каналом (*VirtualLink*).

Для дальнейшей детализации схемы необходимо провести несколько шагов декомпозиции физической связности:

- до уровня соединений между ЦОД;
- до уровня иерархической сетевой модели ЦОД;
- до уровня сегмента ЦОД;
- до уровня конечных сетевых устройств.

После этого необходимо добавить логические уровни для детализации модели:

- канальный уровень, содержащий логику коммутации, виртуальные сети VLAN, VPLS, мосты, коммутаторы L2, очереди, QoS, механизмы multicast, предотвращения петель, безопасности портов, агрегации;
- сетевой уровень, содержащий маршрутизацию, фильтрацию, преобразование адресов;
- транспортный уровень, содержащий фильтрацию, преобразование адресов;
- уровень приложения, содержащий приложения, которые работают с сетью.

Все задачи обеспечения логики работы возлагаются на уровень приложений, остальные уровни лишь содержат необходимую информацию для реализации технологий и протоколов.

Поэтому необходимо представлять подробную схему соединений на каждом уровне декомпозиции. На рисунке 2 показана общая схема соединения ЦОД с указанием некоторых элементов, для верхнего ЦОД указаны сетевые интерфейсы.

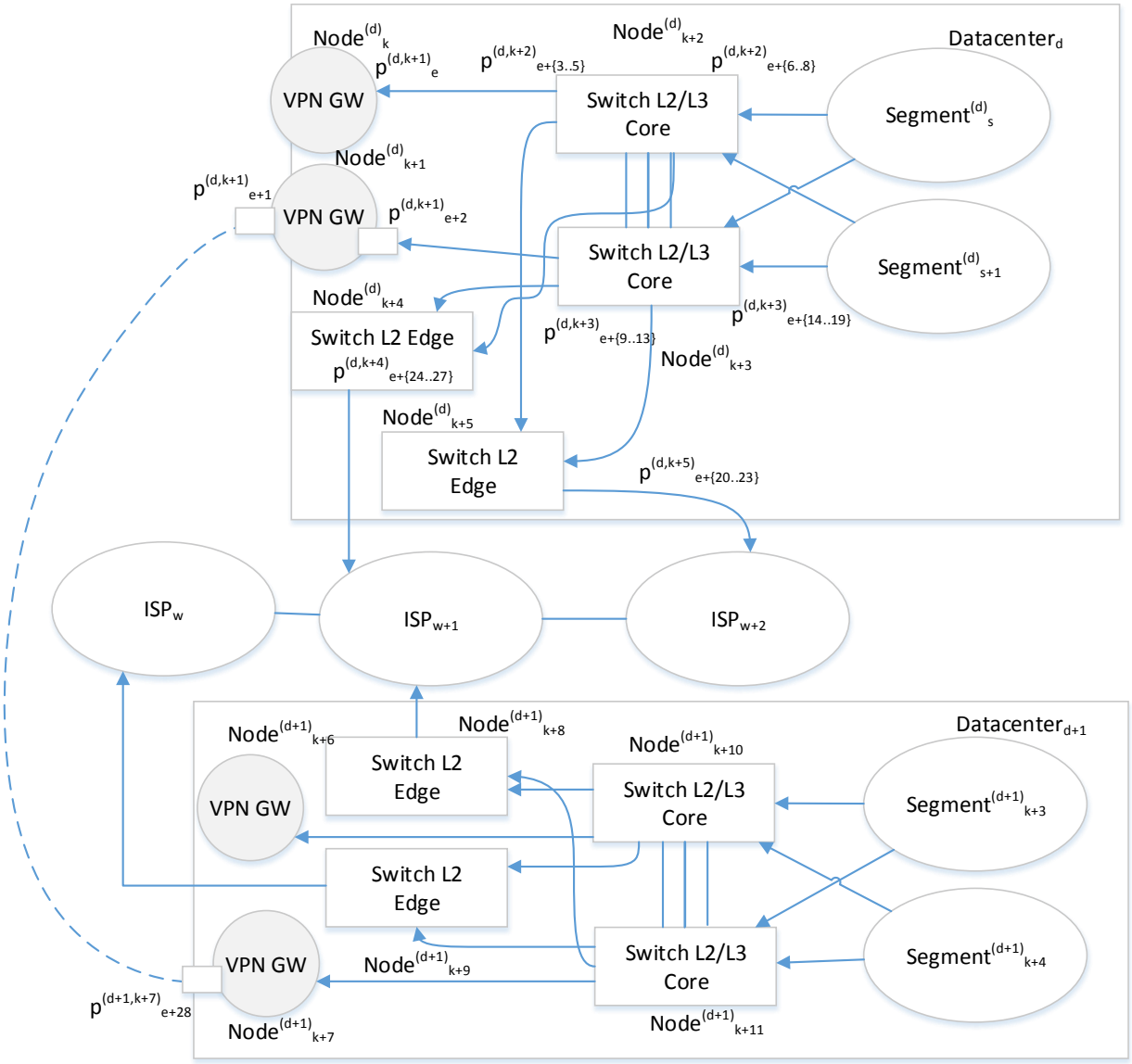


Рисунок 2 – Схема соединений верхнего уровня

Центры обработки данных с помощью граничных VPN шлюзов соединяются друг с другом. Каждая дуга соответствует маршруту между граничными шлюзами двух различных ЦОД. Шлюзы присоединяются к сети провайдеров чаще всего через коммутатор с поддержкой VLAN, в который подключается канал провайдера. Часто один и тот же коммутатор, но разные VLAN и/или порты используются для подключения и канала провайдера и канала в сеть ЦОД.

Внутренняя структура ЦОД может быть представлена в виде аналогичного мультиграфа:

$$Datacenter = (Segments, IntLinks(t)), \quad (2)$$

где вершины $Segments = \{Segment_1, Segment_2, ..., Segment_s\}$ – множество отдельных сегментов (автономных систем, внутренних подсетей, VLAN, VXLAN и других логических сегментов сети) ЦОД, связанных между собой через уровень распределения или ядра сети;

$IntLinks(t) = \{Link_l \cup VirtualLink_l\}$ – дуги, представляющие направленные связи между сегментами. Это результат маршрутизации внутренних сегментов, куда входит, в том числе, маршрутизация BGP, OSPF и L3 коммутация. Программно-конфигурируемая передача данных будет отображаться в L3 коммутацию.

Сегмент $Segment_\xi \in Segments$ вычислительного ЦОД может быть описан в форме взвешенного неориентированного мультиграфа:

$$Datacenter_d \to Segment_\xi = (Datacenter_d \to Node_k, Datacenter_d \to Link_l), \quad (3)$$

где $Node_k$ – вершины, представляющие собой разбиение множеств всех сетевых устройств;

$Datacenter_d \to Links_l = \{(Datacenter_d \to Node_{k1} \to p_i, Datacenter_d \to Node_{k2} \to p_j)\}$ – ребра мультиграфа, представляющие собой двусторонние сетевые связи между портами i и j устройств k1 и k2 сети, причем допускается наличие нескольких параллельных связей между двумя устройствами через разные пары портов или . Поскольку речь идет о конвергентных сетях, связи подсистем хранения также включены в эту структуру;

$Switches = \{Switch_1, Switch_2, ..., Switch_{\max(Switches)}\}$ – множество коммутаторов, в том числе виртуальных;

$Controllers = \{Controller_1, Controller_2, ..., Controller_{\max(Controllers)}\}$ – множество контролеров программно-конфигурируемой сети системы;

$Gateways = \{Gateway_1, Gateway_2, ..., Gateway_{\max(Gateways)}\}$ – множество граничных шлюзов,

$Storages = \{Storage_1, Storage_2, ..., Storage_{\max(Storages)}\}$ – множество хранилищ данных;

$Servers = \{Server_1, Server_2, ..., Server_{\max(Servers)}\}$ – множество серверов;

Логическую структуру сегмента ЦОД можно представить по уровням OSI отдельно:

- уровень 2 (L2) для программно-конфигурируемой сети, VLAN и коммутации;
- уровень 3 (L3) для маршрутизации.

Каждый сетевой порт узла $p_{e1} \in P$ имеет следующие параметры и динамические характеристики:

$$Datacenter_d \to Node_k \to p_{e1} = (Delay, Type, Bandwith, LoadIn(t), LoadOut(t), shutdown(t)) \quad (4)$$

где $Bandwith \in N$ – максимальная пропускная способность передачи порта в кбит/с;

$Delay \in N$ – максимальная пропускная способность передачи порта в кбит/с;

$Type \in \{Media, \mathrm{Protocol}\}$ – тип интерфейса;

$Media = \{"fiber","copper","wireless"\}$ – носитель;

$Protocol = \{"ethernet","infiniband","PON","FC"\}$ – протокол L1.

$LoadIn(t), LoadOut(t) \in [0,1]$ – удельная загрузка исходящей связи порта в момент времени t;

Если порт используется как канальный, то будет присутствовать сущность L2port для хранения параметров L2:

$$Datacenter_d \to Node_k \to p_{e1} \to L2port_{e2} = (MAC, \{Queue(t)\}, \{VLAN(t)\}) \quad (5)$$

где MAC – MAC-адрес;

$\{Q(t)\}$ – набор очередей, ассоциированных с портом, и их состояния в момент времени t;

$\{VLAN(t)\}$ – набор допустимых для интерфейса VLAN, в случае порта доступа – один, со временем могут меняться, особенно в виртуальных средах.

$\{Queue(t)\}$ обозначает набор очередей пакетов, ассоциированных с конкретным портом p_{e1} вычислительного узла $Node_k$. Они используются, чтобы обеспечить согласно QoS минимальную гарантированную пропускную способность и максимальную гарантированную задержку для заданных сетевых связей.

С каждой подобной очередью $Queue(t)$ связаны следующие параметры и динамические характеристики:

$$Queue(t) = (type, \{params\}, MinBand(t), MaxDelay(t)), \quad (6)$$

где $MinBand(t) \in N \cup \{0\}$ представляет собой минимальную пропускную способность (в Кб/с);

$MaxDelay(t) \in N \cup \{0\}$ – максимальная задержка для соответствующей очереди порта (в мкс), которая была установлена механизмом обеспечения QoS;

$type = \{"CBQ","PQ","CQ","CBFQ","LLQ","WRR","WRED"\}$ – тип очереди;

{params} – набор параметров, для каждого типа очереди свой набор, общим является размер очереди.

Виртуальная сеть канального уровня определяется как набор интерфейсов на канальном уровне:

$$Datacenter_d \to vNet(t) = \{L2Link_{e2}\} \quad (7)$$

Openflow потоки данных внутри сегмента ЦОД можно представить в виде взвешенного неориентированного мультиграфа такого вида:

$$Datacenter_d \to Segment_\xi \to OFlows(t) = \{OFlow_i(t)\} \quad (8)$$

– набор потоков, появившихся в сегменте $Segment_\xi$ к моменту времени t.

Поток $OFlow_i(t)$ может быть описан следующим образом:

$$OFlow_i(t) = (SrcIP, SrcMAC, DestIP, DestMAC, TimeOut, MinGarantBand, MaxGarantDelay, path(t), t(t), s(t)), \quad (9)$$

где $SrcIP$ – IP-адрес источника потока;

$SrcMAC$ – MAC-адрес источника потока;

$DestIP$ – IP-адрес получателя потока;

$DestMAC$ –MAC-адрес получателя потока;

$TimeOut$ – время, на которое установлена запись о потоке;

$MinGarantBand$ – минимальная гарантированная пропускная способность потока;

$MaxGarantDelay$ – максимальная гарантированная задержка потока;

$path(t)$ – динамическая характеристика пути на момент времени t, по которому спланирован поток;

$t(t)$ – предыдущий момент времени, когда обрабатывался хотя бы один пакет потока;

$s(t) \in \{"created", "dropped'\}$ – состояние потока на момент времени t.

Путь на соответствующем уровне модели (L1, L2, L3) может быть определен в виде совокупности портов:

$$L1Path(t) = (p_1, p_2, ..., p_e) \quad (10)$$

$$L2Path(t) = (L2port_1, L2port_2, ..., L2port_e) \quad (11)$$

$$L3Path(t) = (L3port_1, L3port_2, ..., L3port_e) \quad (12)$$

Итоговый путь может содержать объединение всех видов путей или только некоторые, при этом если используется *L2Path,* то *L1Path* можно получить через наследование *L2port* от *p*:

$$path(t) = \{L1Path\} | \{L2Path\} | \{L3Path\} \quad (13)$$

Такой подход в случае, если два сетевых устройства имеют несколько параллельных связей, позволяет указывать конкретную связь, входящую в путь. Если получатель и отправитель потока находятся внутри одного сегмента, то путь полностью проходит внутри него. Если получатель потока находится в другом сегменте, то путь ведет к одному из граничных шлюзов, имеющих префикс целевого сегмента. В случае, когда отправитель потока находится в другом сегменте, то путь прокладывается от граничного шлюза к получателю.

Каждый вычислительный узел $Node_k \in Nodes$ характеризуется следующими параметрами и динамическими характеристиками:

$$Node_{ki} = (M\ , D\ , C\ , S\ , P, m\ (t), d\ (t), u\ (t), s(t)) \qquad (14)$$

где $M\ \in N$ – размер его оперативной памяти в мегабайтах;

$D\ \in N$ – размер его дисковой памяти в мегабайтах;

$C\ \in N$ – количество его вычислительных ядер;

$S \in R^{+}$ – величина их производительности относительно самого медленного ядра во всем распределенном ЦОД;

$P = \{p_e\}$ – множество сетевых портов;

$m\ (t) \in [0,1]$ – удельная доля загруженности оперативной памяти вычислительного узла в момент времени t;

$d(t) \in [0,1]$ – удельная доля загруженности дисковой памяти вычислительного узла в момент времени t;

$u\ (t) = (u_1(t), u_2(t), ..., u_{\max(u)}(t))$ – вектор загруженностей каждого из вычислительных ядер узла в момент времени t, причем $u\ (t) \in [0,1]$;

$s(t) \in \{"online","offline"\}$ – состояние вычислительного узла в момент времени t.

Все вычислительные узлы являются SMP-узлами, состоящими из однотипных многоядерных процессоров. Вычислительные ядра могут относиться как к отдельным процессорам (по одному ядру на каждом), так и к нескольким многоядерным процессорам. Они рассматриваются, как единое множество равноправных и симметричных вычислительных ядер узла $Node_k$. Данные ядра разделяют общую оперативную память размера M и дисковую память размера D, а также способны обмениваться данными с другими вычислительными узлами через сетевую подсистему.

Тип сетевого узла *Server* имеет особенность – возможность запуска виртуальных машин, контейнеров, контейнеров в виртуальных машинах, которые являются сетевыми узлами и, соответственно, имеют сетевые интерфейсы. Для работы виртуальных машин требуются виртуальные коммутаторы, которые также являются сетевыми узлами и имеют интерфейсы. Серверы содержат компоненты (приложения) для доступа к системам хранения, оркестраторы, контроллеры. Эти элементы будут использованы при описании конкретных приложений или систем доступа. На рисунке 3 показан пример схемы сервера.

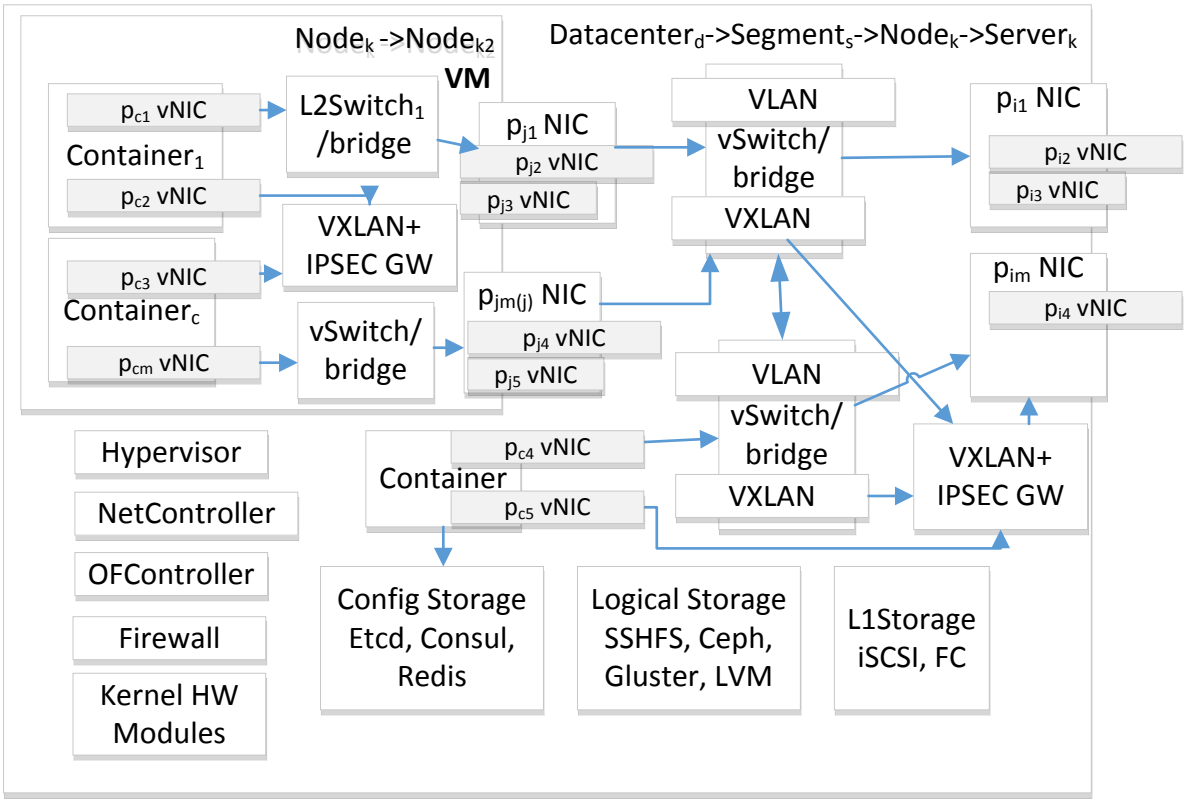


Рисунок 3 – Пример схемы сервера

Сетевые хранилища содержат образы экземпляров виртуальных машин, вычислительные задачи, базы данных приложений, а также инфраструктурные компоненты вычислительного облака. В системах обработки больших данных обычно содержатся элементы HDFS.

Каждое хранилище $Storage_k \in Storages$ сегмента $Segment_s$ имеет следующие параметры и динамические характеристики в дополнении к *Node*:

$$Storage_k = (MaxVolume, Volume(t), \overline{R}(t), \overline{W}(t))$$

где $MaxVolume \in N$ – максимальный объем хранилища в килобайтах;

$Volume(t) \in N \cup \{0\}$ – доступный объем хранилища в килобайтах в момент времени t;

$\overline{R}(t)$ – средняя установившаяся к моменту времени t скорость чтения данных;

$\overline{W}(t)$ – средняя установившаяся к моменту времени t скорость записи данных.

Коммутаторы L3 *Switch* имеют в дополнении к модели узла компоненты очередей, различных фильтров, интерфейсы всех видов, в том числе вложенные (например, логический интерфейс для задания адреса на VLAN). Схема такого коммутатора показана на рисунке 4.

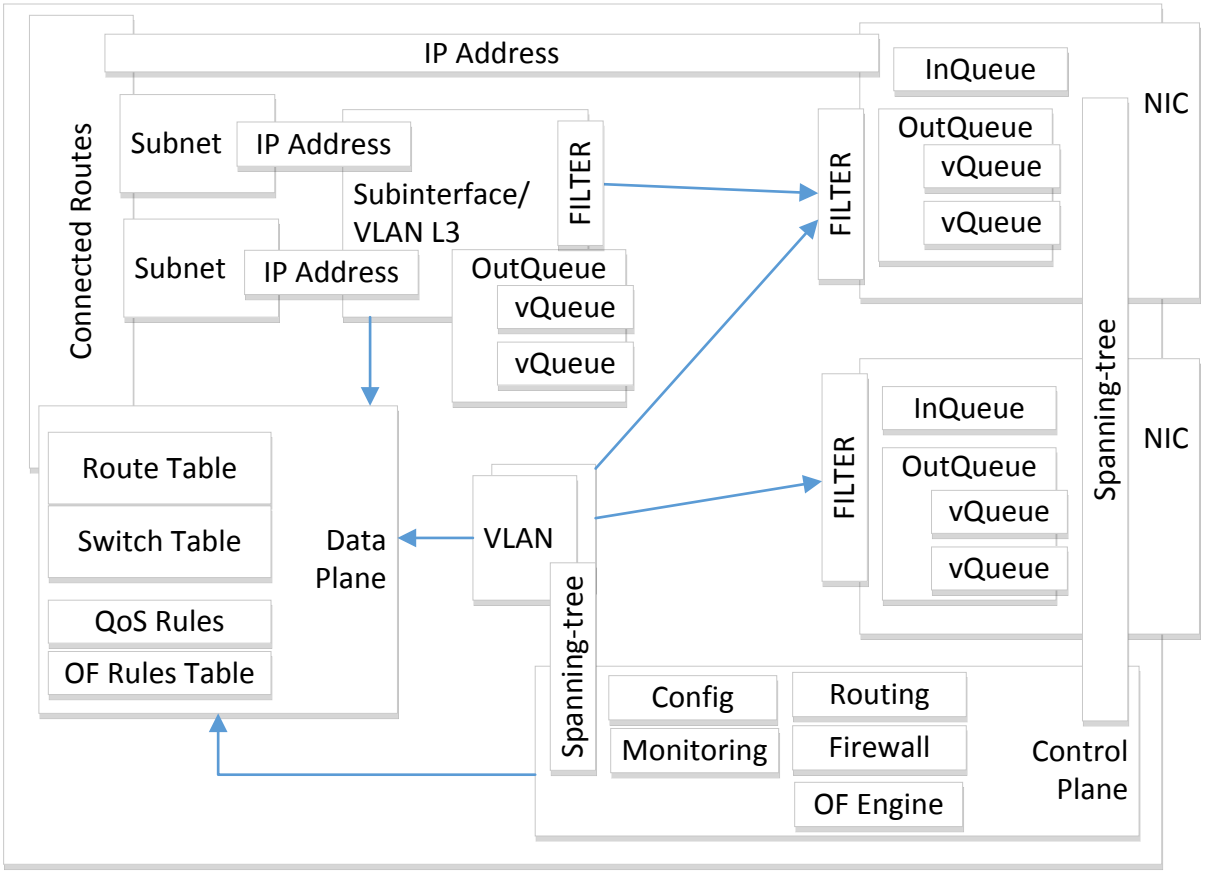


Рисунок 4 – Пример схемы коммутатора

Разработанная структурная модель распределённого ЦОД позволяет формализовать структуру нескольких ЦОД в виде ориентированного взвешенного мультиграфа его сегментов, каждый сегмент определяется в виде неориентированного взвешенного мультиграфа сетевых устройств, к которым относятся: вычислительные узлы, коммутаторы, контроллеры облака, граничные шлюзы, балансировщики коммутаторов и сетевые хранилища.

Для реализации автоматизации распределенных вычислений для обработки больших данных необходимо описать структуру одного сегмента, поверх которой разворачивается комплекс приложений Hadoop, поверх которого работает диспетчер YARN, с которым взаимодействует фреймворк Spark, в котором реализуется конкретный функционал. Данные хранятся в вычислительных узлах с системой хранения, поверх которой реализовано хранилище HDFS, поверх которой используется один из совместимых способов хранения данных, например HBase или чистая система HDFS.

На рисунке 5 показана схема соединений сегмента ЦОД. Для реализации Hadoop важно то, что в ней выделены коммутаторы стоек TOR(Top Of Rack) и их соединение с основной сетью и системой хранения. В большинстве случаев недорогие, но конвергентные решения используют соединения iSCSI с системой хранения, более производительные системы используют FC.

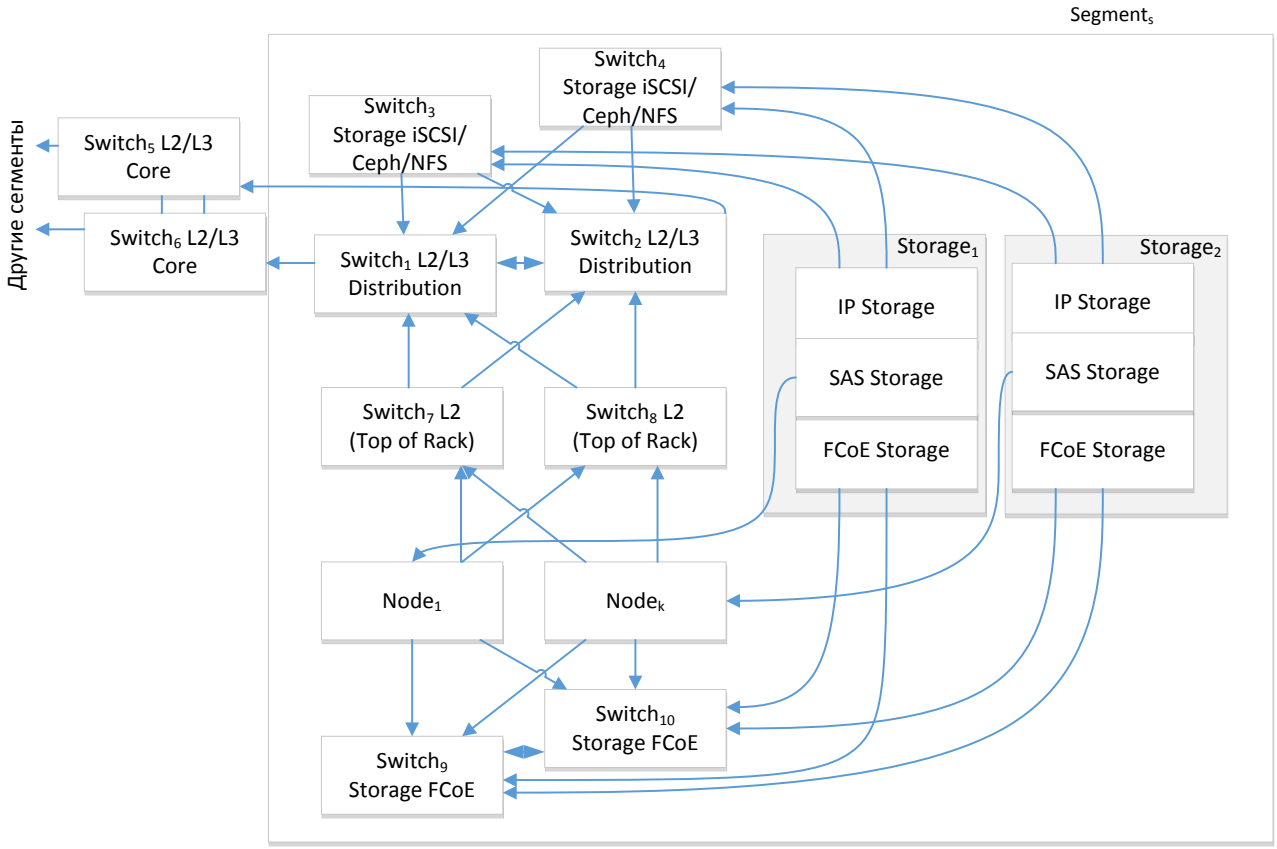


Рисунок 5 – Структура сегмента ЦОД

Сегмент представлен стандартной архитектурой Ядро-Распределение-Доступ для ЦОД, в нем содержится еще подсистема хранения, а уровень доступа использует минимум два соединения к каждому серверу.

На рисунке 6 показана схема работы платформы обработки больших данных. На нижнем уровне располагаются подсистема хранения и подсистема выполнения, размещенная на узлах. Подсистемой хранения управляет NameNode и система размещения данных HDFS. Узлы хранения могут быть совмещены с узлами выполнения, но это не рекомендуется для больших данных из-за высоких накладных расходов на работу системы хранения. Узлы выполнения имеют запущенный сервис-мастер, который при получении задания на размещение в контейнер приложения обращается к ресурсному менеджеру для выделения ресурсов на узле, и запускает приложение. Прямой доступ к системе хранения обеспечивает более высокую производительность, для приложений, поддерживающих WebHDFS, имеется отдельный модуль взаимодействия через REST API.

Ключевым элементом для взаимодействия всех внутренних компонентов системы является система централизованного хранения и взаимодействия ZooKeeper, через которую компоненты находят друг друга, считывают конфигурацию и синхронизируются.

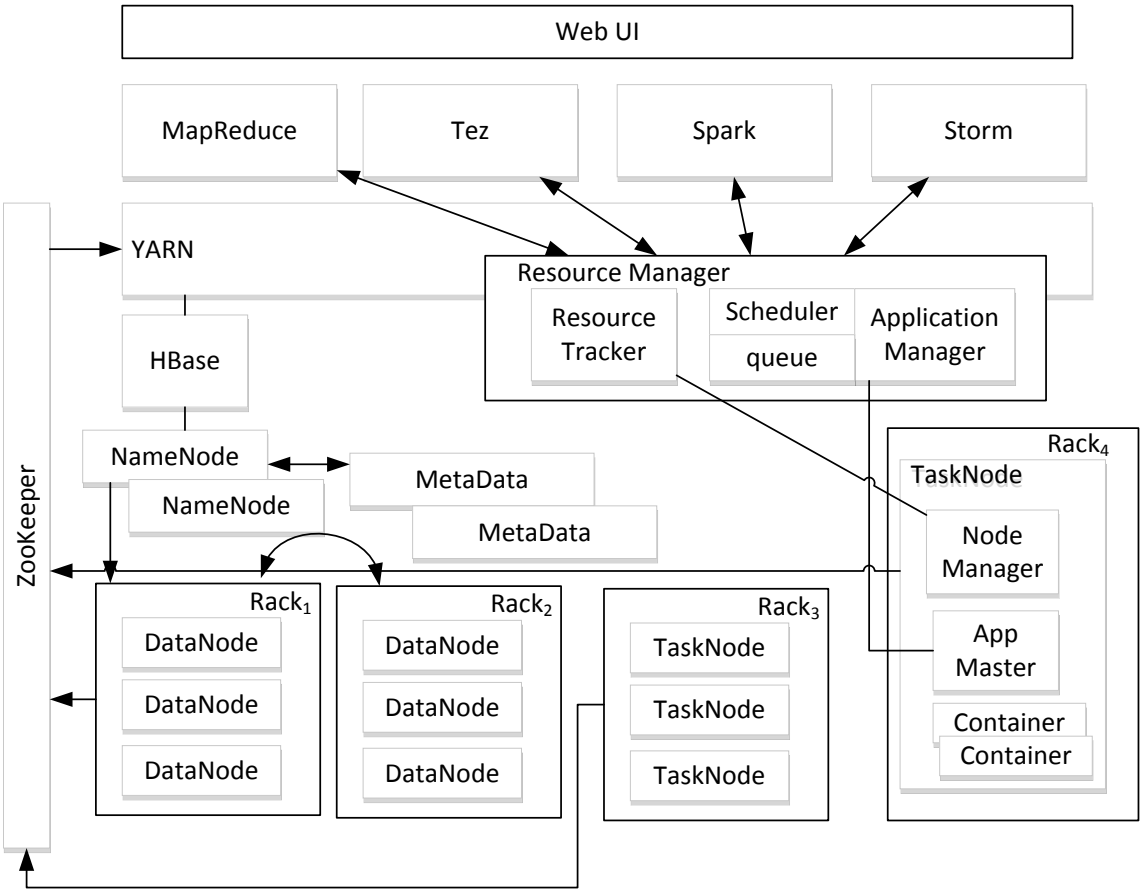


Рисунок 6 – Платформа автоматизации обработки больших данных

Таким образом, в рамках статьи разработана комплексная модель для исследования работы распределенных систем обработки больших данных. Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 18-07-01446, 18-47-560017, и 18-37-00460.

ПРИМЕНЕНИЕ ЗАДАЧИ ОБУЧЕНИЯ С ОШИБКАМИ В ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Фадеев С.В.
Оренбургский государственный университет

Обучение с ошибками (LWE) – концепция, подразумевающая намеренное введение ошибки в простые вычисления с целью затруднения их решения известными методами. Была представлена Одедом Регев в 2005 году и сразу вызвала интерес как основа для построения криптографических средств, устойчивых к криптоанализу с использованием квантовых компьютеров. Такая устойчивость обусловлена сведением задачи обучения с ошибками к проблеме решеток, являющейся одним из основных направлений постквантовой криптографии.

Описание задачи

Определяется параметр $n \geq 1$, модуль $q \geq 2$ и распределение вероятности ошибки χ на Z_q.

Пусть $A_{s,\chi}$ — соотношение векторов на $\mathbb{Z}_q^n \times \mathbb{Z}_q$, полученное случайным выбором вектора $a \in \mathbb{Z}_q^n$, выбором ошибки $e \in \mathbb{Z}_q^n$ в соответствии с χ и полученным выражением

$$(a,\ a, s\ + e), \tag{1}$$

где

$$a, s\ =\ \ {}^{n}_{i=1}\, a_i s_i \tag{2}$$

и сложение производится по модулю q. Алгоритм решает задачу $LWE_{q,\chi}$, если для любого секрета $s \in \mathbb{Z}_q^n$, имея произвольное число независимых соотношений из $A_{s,\chi}$ он с высокой вероятностью выдаст s.

Пример: найти вектор s.

$$\begin{gathered} 14s_1 + 15s_2 + 5s_3 + 2s_4 \approx 8(mod17) \\ 13s_1 + 14s_2 + 14s_3 + 6s_4 \approx 16(mod17) \\ 6s_1 + 10s_2 + 13s_3 + s_4 \approx 3(mod17) \\ 10s_1 + 4s_2 + 12s_3 + 16s_4 \approx 12(mod17) \\ 9s_1 + 5s_2 + 9s_3 + 6s_4 \approx 9(mod17) \\ 3s_1 + 6s_2 + 4s_3 + 5s_4 \approx 16(mod17) \\ \dots \\ 6s_1 + 7s_2 + 16s_3 + 2s_4 \approx 3(mod17) \end{gathered}, \tag{3}$$

где каждое уравнение верно до некоторой ошибки (± 1). Ответ: $s = (0,13,9,11)$. Если бы в примере отсутствовала ошибка, s можно было бы восстановить за полиномиальное время. Например, алгоритм исключения Гаусса принимает линейные комбинации n уравнений, тем самым усиливая погрешность до неуправляемых уровней, не оставляя по существу никакой информации в полученных уравнениях.

Отметим, что можно рассматривать LWE как проблему декодирования из случайных линейных кодов или как задачу случайного ограниченного расстояния для декодирования. Кроме того, было доказано, что задача обучения с ошибками может быть сведена к задачам, относящимся к теории решеток, являющихся *NP*-сложными, что сразу повлекло разработку криптографических приложений.

Теория решеток

Решеткой называется множество точек в -мерном пространстве с периодической структурой, заданное n-линейно независимыми векторами $b_1, \dots, b_n \in \mathbb{R}^n$, называемыми базисом решетки:

$$\mathcal{L}\ b_1, \dots, b_n\ = \ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z}\ . \qquad (4)$$

Криптосистемы на решетках строятся исходя из предположения, что не существует полиномиального квантового алгоритма, который аппроксимирует решетчатые задачи с точностью до полиномиальных факторов.

Базис может быть представлен матрицей $B = \ b_1, \dots, b_n\ \in \mathbb{R}^{n*n}$, имеющей базисные векторы в виде столбцов. Используя матричную запись, решетка, порожденная матрицей B, может быть определена как

$$\mathcal{L}\ B\ = \ BX,\ X \in \mathbb{Z}\ , \qquad (5)$$

где BX - обычное умножение матрицы на вектор.

Если U - унимодулярная матрица (т. е. целочисленная квадратная матрица с определителем ± 1), то B и BU порождают одну и ту же решетку. Т.о., любая решетка допускает множество оснований, и этот факт лежит в основе многих криптографических приложений. Определителем решетки является абсолютная величина определителя базисной матрицы:

$$\det(\mathcal{L}\ B)\ = |det\ B\ |. \qquad (6)$$

Значение детерминанта не зависит от выбора базиса и геометрически соответствует обратному значению плотности точек решетки в $\mathbb{R}^n$.

Проблемы, основанные на решетках:

– Задача Нахождения Кратчайшего Вектора (SVP): заданный базис решетки B, найти самый короткий ненулевой вектор в $\mathcal{L}\ B$.

– Ближайшая Векторная Задача (CVP): заданный решеточный базис B и целевой вектор t (не обязательно в решетке), найдите ближайшую к t точку решетки $v \in \mathcal{L}\ B$.

– Задача Нахождения Независимого Вектора (SIVP): задан базис решетки $B \in \mathbb{Z}^{n*n}$, найти n линейно независимых решеточных вектора

$$S = \ s_1, \dots, s_n \ , \qquad (7)$$

где $s_i \in \mathcal{L}\ B$),
минимизируя величину

$$S \ = max_i \ s_i \ . \qquad (8)$$

В криптографии на основе решеток обычно рассматривается аппроксимационный вариант этих задач, который обозначается дополнительным индексом γ, указывающим коэффициент аппроксимации. Например, в SVPγ цель состоит в том, чтобы найти вектор, норма которого не более, чем в γ раз больше, чем у кратчайшего ненулевого вектора.

В 2005 году Одед Регев доказал, что задача обучения с ошибками сводится к модификациям задачи нахождения кратчайшего вектора и задачи нахождения независимого вектора, а в 2009 Крис Пейкер смог свести ее к одной задаче нахождения кратчайшего вектора в отношении стойкости к классическому и квантовому криптоанализу.

Квантовый криптоанализ

Квантовый криптоанализ – взлом криптосистем, подразумевающий использование для этих целей квантового компьютера и квантовых алгоритмов. Квантовый компьютер, ввиду своего быстродействия, позволяет решать множество вычислительно сложных задач за приемлемое время, что стимулировало поиск криптосистем с доказанной математической стойкостью.

В основе работы квантового компьютера лежат принципы квантовой механики, в частности квантовая суперпозиция - понятие, подразумевающее нахождение системы в некотором состоянии, объединяющем несколько взаимоисключающих состояний.

Математически суперпозиция представляется как сумма произведений базисных состояний на их комплексные амплитуды:

$$|\psi \ = \ \sum_{j=0}^{N-1} \lambda_j \, |j \ , \qquad (9)$$

где $|\psi\ -$ суперпозиция;

$\lambda_j -$ комплексная амплитуда;

$|j\ -$ базисное состояние.

Квантовый параллелизм: при вычислении суперпозиции осуществляются операции одновременно над всеми базисными состояниями. Таким образом, обеспечивается значительный рост производительности систем, построенных на квантовых принципах. Некоторые трудности возникают при извлечении данных из базисных состояний. Ввиду этого в архитектуре квантовых вычислительных систем выделяют два представления, в которых может находиться квантовое состояние:

– операция – это последовательность унитарных операций (квантовых вентилей), осуществляемых над состоянием;

– измерение – это присвоение состоянию суперпозиции некоторого его базисного состояния в соответствии с вероятностью, определяемой комплексной амплитудой.

Квантовая запутанность – это явление наличия между парой элементарных частиц определенной связи: обе находятся в противоположных состояниях при выходе из суперпозиции, при измерении одной из них соответственно изменяется и другая, независимо от расстояния между ними.

Основой квантовых компьютеров являются кубиты – разряды для хранения информации, принимающие значения: одно из двух противоположных или их суперпозицию, то есть:

$$\psi\ = \alpha\ 0\ + \beta|1\ , \qquad (10)$$

где $\alpha, \beta \in \mathbb{C}$: $\alpha\ ^2 + \ \beta\ ^2 = 1.$

Применение кубитов и обуславливает высокую производительность (экспоненциальную) квантовых компьютеров, так как использование L таких кубитов в регистре равносильно наличию в системе 2^L классических состояний.

Значительными препятствиями в разработке квантовых систем являются некоторые слабо изученные механизмы квантовой механики, такие, например, как редукция фон Неймана – мгновенное изменение квантового состояния объекта, происходящее при измерении. Таким образом, создаются множественные ошибки в регистрах. Противодействием этому является применение охлаждения жидким гелием, что существенно усложнит конструкцию и затруднит эксплуатацию перспективных квантовых компьютеров. Большую роль играет и организация управления каждым кубитом индивидуально. Подобные задачи требуют прецизионно выполненного управляющего компонента. Эти, а также многие другие проблемы, затрудняют масштабируемость многих проектов квантовых компьютеров.

Технологиями, пригодными для квантовых компьютеров на данный момент, считаются:

1) твердотельные квантовые точки на полупроводниках: в качестве логических кубитов используются зарядовые состояния или направление электронного, или ядерного спина, управление внешними потенциалами или лазерным импульсом;

2) сверхпроводящие элементы: присутствие/отсутствие куперовской пары в определённой области пространства, управление: внешний потенциал или магнитный поток;

3) ионы в вакуумных ловушках Пауля или атомы в оптических ловушках, в качестве логических кубитов используются основное или возбуждённое состояния внешнего электрона в ионе, управлением служат колебательные моды ионного ансамбля или лазерные импульсы;

4) смешанные технологии: использование заранее приготовленных запутанных состояний фотонов для управления атомными ансамблями или как элементы управления классическими вычислительными сетями.

За последнее время было представлено значительное количество новых разработок.

1) 14 июля 2017 года в Гарварде был представлен 51 кубитный квантовый компьютер разработки группы Михаила Лукина, работающий на основе применения холодных атомов рубидия в случайном состоянии в оптических ловушках.

2) 13 ноября 2017 года представлен 50 кубитный компьютер IBM. Квантовые эффекты обеспечиваются использованием сверхпроводников, время устойчивой суперпозиции составляет до 90 миллисекунд.

3) 29 ноября 2017 года университет Мерилэнда представил 53 кубитный компьютер Кристофера Монро, применяющий ионы иттербия-171 в оптических ловушках, используя в качестве значений направления их спинов

4) 6 марта 2018 года представлен 72 кубитный компьютер компании Google, основанный на сверхпроводящих элементах, выстроенных в две противолежащие матрицы 6*6. Подчеркивается рекордно высокая надежность: вероятность возникновения ошибки однокубитного вентиля в 0,1%, двухкубитного – в 0,6%.

5) Компания Intel, совместно с Нидерландами, работает в двух направлениях: в январе 2018 года представлен 49 кубитный чип Tangle Lake, на сверхпроводящих элементах; в июне 2018 представлен чип на спиновых кубитах рекордно малого размера – до 50 нм, использующий технологии, производные от производства транзисторов.

Уже сейчас квантовые компьютеры позволяют работать в направлениях квантовой химии и изучения квантовой механики, криптоанализ же требует значений разрядности квантовых чипов в несколько сотен тысяч кубитов, но при этом она является одной из ключевых задач создания квантовых компьютеров, что выражается в объемах спонсирования программ со стороны соответствующих управлений государств. Экспертные оценки, с учетом

доказанной в настоящее время возможности масштабируемости квантовых компьютеров, позволяют предполагать появление таких компьютеров к середине-концу следующего десятилетия. Показательным также является урезание в этой связи расходов на переход инфраструктуры с RSA на считавшуюся перспективной эллиптическую криптографию.

Квантовый компьютер не способен решать новые типы задач, отличные от решаемых классическими компьютерами, но, благодаря применению кубитов, достигнут существенный рост производительности вычислений обычных. Это позволяет проектировать алгоритмы, в наибольшей степени использующих данную особенность.

Такие перспективы стимулировали появление квантовых алгоритмов, одним из которых являлся алгоритм Шора – алгоритм решения задачи факторизации, а затем и задачи дискретного логарифмирования (основных проблем, на которых базируется криптография с открытым ключом). Представленный в 1994 году, он спровоцировал интерес к развитию отрасли. Будучи основан на квантовом преобразовании Фурье (расширение дискретного преобразования Фурье на использование квантового компьютера), он стал первым квантовым алгоритмом криптоанализа. В 2001 году была практически продемонстрирована возможность факторизации числа 15 на 7 кубитном компьютере этим алгоритмом.

Последовавший затем алгоритм Гловера, осуществляющий поиск в базах данных за квадратичное время, продемонстрировал возможность взлома и симметричных криптосистем.

Применение проблемы обучения с ошибками в ЭЦП

Проблема LWE находит применение в конструировании криптоалгоритмов симметричного и ассиметричного шифрования, протоколов распределения ключей, хэш-функций и схем электронно-цифровой подписи. Схема ЭЦП на этой проблеме была впервые представлена Любашевским в 2011 году и пережила несколько модернизаций.

Алгоритм:

Операции производятся в конечном поле $\mathbb{F}_q$, где $q -$ нечетное простое число. Случайным образом задается полином $a\ x$ вида: $a\ x\ = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$.

Генерация ключей:

1) создаются два полинома, служащие закрытым ключом, $s_0\ x$ и $s_1(x)$ с коэффициентами, выбранными равномерно из множества $-\frac{(q-1)}{2}, 0, \frac{(q-1)}{2}$.

2) вычисляется открытый ключ:

$$t\ x\ = a\ x\ \cdot s_0\ x\ \ + s_1\ x\ . \qquad (11)$$

Создание подписи:

1) создаются два полинома, $y_0\ x\ $ и $y_1(x)$ с коэффициентами, выбранными равномерно из множества $-\frac{(q-1)}{2}, 0, \frac{(q-1)}{2}$.

2) вычисляется:

$$\mathrm{w}\ \mathrm{x}\ = \mathrm{a}\ \mathrm{x}\ \cdot y_0\ x\ \ + y_1\ x\ . \qquad (12)$$

3) w x переводится в битовое представление ω.

4) вычисляется хэш-функция POLYHASH, принимающая на вход битовую строку, выдающую полином из n коэффициэнтов, k из которых ненулевые и меньше значения диапазона выбора коэффициентов полиномов.

$$\mathrm{c}\ (\mathrm{x})\ =\ \mathrm{POLYHASH}\ (\omega \mid \mathrm{m}). \qquad (13)$$

5) вычисляется:

$$z_0\ x\ \ =\ s_0\ x\ \ \cdot \mathrm{c}\ (\mathrm{x})\ +\ y_0\ x\ . \qquad (14)$$

6) вычисляется:

$$z_1\ x\ = s_1\ x\ \cdot \mathrm{c}\ (\mathrm{x}) + y_1\ x\ . \qquad (15)$$

До тех пор, пока равномерные нормы (т.е., значение наибольшего коэффициента полинома) $z_0\ x\ $ и $z_1\ x\ \leq \beta$ (т.е. разность диапазона выборки и числа ненулевых коэффициентов), осуществляется переход к первому шагу.

Под подписью понимается тройка многочленов: $\mathrm{c}(\mathrm{x})$, $z_0\ x\ $ и $z_1\ x\ $.

Проверка подписи:

1) проверяется, что равномерные нормы $z_0\ x\ $ и $z_1\ x\ \leq \beta$.

2) вычисляется

$$\mathrm{w}'(\mathrm{x})\ =\ \mathrm{a}\ (\mathrm{x})\ \cdot z_0\ x\ + z_1\ x\ - t\ x\ c(x) \qquad (16)$$

3) w′ x переводится в битовое представление ω'

4) вычисляется:

$$\mathrm{c}\ '(\mathrm{x})\ = POLY\mathrm{HASH}\ (\omega' \mid \mathrm{m}). \qquad (17)$$

Если $c\ x\ = c'\ x\ $ – подпись действительна и можно удостовериться в целостности, авторстве и неотказуемости от авторства, если нет – недействительна.

В сравнении с другими постквантовыми алгоритмами ЭЦП (основанными на хэш-функциях, кодах исправления ошибок и многомерных квадратичных системах), схемы на основе задачи обучения с ошибками демонстрируют малые размеры открытого ключа при относительно небольшой длине подписи. Множество приложений, математическая доказуемость, преимущества перед другими ЭЦП и приемлемость создания реализаций позволяют расценивать ЭЦП на основе задачи обучения с ошибками как очень перспективное направление.

Список литературы

1 Peter W. Shor, Algorithms for quantum computation: discrete logarithms and factoring // SFCS '94 Proceedings of the 35th Annual Symposium on Foundations of Computer Science, November 20 - 22, 1994, IEEE Computer Society Press. – 1994 – С.124-134.

2 Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, Post-Quantum Cryptography / Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen; Springer-Verlag. – Berlin, 2009. – С. 245. – ISBN: 978-3-540-88701-0.

3 Oded Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography// STOC '05 Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, Baltimore, MD, USA — May 22 - 24, 2005, – С. 84-93. - ISBN:1-58113-960-8.

4 Oded Regev, The Learning with Errors Problem// 2012 IEEE 27th Conference on Computational Complexity (2010), - Boston, Massachusetts, June 9-12, 2010, - ISBN: 978-0-7695-4060-3.

5 Vadim Lyubashevsky, Chris Peikert, Oded Regev, A Toolkit for Ring-LWE Cryptography// Extended abstract appears in Eurocrypt 2013, Springer, Berlin, Heidelberg, - 16 May 2013, - С. 35-54, - ISBN 978-3-642-38347-2.

6 Cryptology ePrint Archive [Электронный ресурс].: Johannes Buchmann, Carlos Coronado, Martin Doring, Daniela Engelbert, Christoph Ludwig, Raphael Overbeck, Arthur Schmidt, Ulrich Vollmer, Ralf-Philipp Weinmann, Post-Quantum Signatures, 2004 – Режим доступа: http://eprint.iacr.org/2004/297.pdf/. – 20.09.2018.

ОБЗОР ИСТОЧНИКОВ ПО ТЕМЕ МОНИТОРИНГА МОБИЛЬНЫХ ОБЪЕКТОВ

Фаткуллина Р.Р.
Оренбургский государственный университет

На сегодняшний день расширяется список сфер человеческой деятельности, в которых активное участие принимает мониторинг мобильных объектов: технологии позиционирования объектов активно используются в государственной сфере, в работе всего транспортного комплекса, всех его отраслей. Навигация различных мобильных объектов стала повсеместной: системы диспетчеризации и мониторинга, логистики, обеспечения безопасности, интеллектуальные транспортные системы, тахографический контроль работают с применением спутниковой навигации.

Целью статьи является проведение обзора современных публикаций по теме мониторинга мобильных объектов по следующим характеристикам: цель статьи, подходы к решению, рассматриваемые в статье; результаты.

Среди публикационных работ по тематике мониторинга мобильных объектов следует отметить следующие статьи:

1. Аралбаев Т.З. Исследование погрешностей в системе мониторинга мобильных объектов на основе навигационного ключа /Аралбаев Т.З., Галимов Р.Р., Идрисов А.Ш., Каменева Е.В., Солдатов А.С.// Сборник статей XIII международной научно-практической конференции «Прогрессивные технологии в транспортных системах», 2017. – С. 9-12 [1].

Целью статьи является определение и уточнение характера изменения погрешностей используемых навигационных средств на практике, в частности в условиях города Оренбурга.

Подходы: проведение эксперимента по исследованию погрешностей используемых навигационных средств.

Результаты работы: на основе проведенного исследования погрешности навигационного оборудования, применяемого в системе мониторинга мобильных объектов на основе навигационного ключа, были определены такие параметры, как: погрешность и радиус разброса навигационных координат, а также радиус диапазона действия навигационного ключа.

2. Григорьевский В.И. Мобильные приемо - передающие устройства для системы позиционирования в задачах контроля наземных объектов /В.И. Григорьевский// Измерительная техника, №5. - 2013. – С. 10-13 [2].

Целью статьи является построение автономной системы позиционирования объектов без привлечения спутниковых навигационных систем.

Подходы: в качестве основного подхода к решению проблемы взято использование инфраструктуры мобильной связи.

Результаты исследования: Рассмотрена проблема построения автономной системы позиционирования объектов при использовании инфраструктуры

мобильной связи без постоянного привлечения спутниковых навигационных систем.

3. Карпик А.П. Навигационно - информационная система точного позиционирования транспорта с использованием наземной инфраструктуры ГЛОНАСС /Карпик А.П., Ганагина И.Г., Косарев Н.С., Голдобин Д.Н.// Журнал «Гироскопия и навигация», №2. - 2015. – С. 47-57 [3].

Целью статьи является описание функционала и рассмотрение работы варианта навигационно - информационной системы точного позиционирования транспорта с использованием бюджетной ГНСС - аппаратуры и наземной инфраструктуры ГЛОНССС.

Подходы: в качестве основного подхода к решению проблемы взято комплексное применение аппаратуры глобальной навигационной спутниковой системы и аппаратура потребителя на дециметровом уровне точности.

Результаты исследования: Система носит завершенный характер, состоит из структурно дополняющих друг друга блоков и обеспечивает дециметровую точность позиционирования.

4. Каширская Е.П. Об алгоритме решения задачи определения координат текущего местоположения по телеметрической информации /Е.П. Каширская// Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника», №1. – 2014. – С. 106 – 109 [4].

Целью статьи является исследование величины расхождений параметров движения, полученные при сравнении действительных и рассчитанных значений.

Подход: сравнение действительных значений и рассчитанных традиционным методом решения в параметрах Эйлера – Крылова с датчикопреобразующей аппаратуры невысокой точности на интервалах движения объекта.

В результате статьи определено, что рост ошибок расчета параметров движения объектов, является следствием накопления погрешностей от сбойной информации, а в качестве недостатков метода в параметрах Эйлера – Крылова следует отметить нелинейность кинематических уравнений.

5. Сарайкин А. И. Позиционирование мобильного объекта на дорожном полотне в условиях дефицита информации /Сарайкин А. И., Аралбаев Т. З., Хасанов Р. И.// Вестник Оренбургского государственного университета, №4. - 2015. – С.114-118 [5].

Целью статьи является повышение активной безопасности мобильного объекта на основе навигационных методов и средств информационной поддержки водителей.

Основным подходом для решения поставленной цели стала разработка прототипа системы, включающего функциональные модули сбора, регистрации и обработки данных о траектории движения мобильного объекта.

Результаты исследования показали, что на основе выбранного подхода поддерживается повышение активной безопасности мобильного объекта в условиях дефицита информации.

6. Хасанов Р. И. Инструментальная база для исследования режима позиционирования мобильного объекта в условиях дефицита информации /Хасанов Р. И., Сарайкин А. И., Аралбаев Т. З.// Журнал автомобильных инженеров, №1. - 2015. – С. 5 – 9 [6].

Целью статьи является повышение активной безопасности мобильных объектов в условиях дефицита информации на основе новых методов и средств информационной поддержки водителей.

Подходы: в качестве основного подхода к решению проблемы повышения активной безопасности мобильных объектов в условиях дефицита информации разработан пакет прикладного программного обеспечения.

Результаты исследования: Разработана и представлена инструментальная база в виде пакета прикладных программ для исследования режима позиционирования и мобильного объекта на дорожном полотне в условиях дефицита информации. Выводы: разработанный комплекс программ позволит решить вопросы позиционирования мобильных объектов в условиях дефицита информации.

7. Хасанов Р. И. Модифицированный «V2V» подход позиционирования мобильных объектов как средство снижения аварийности машин скорой помощи /Р. И. Хасанов// Альманах молодой науки, №2. - 2016. - С. 12 – 14 [7].

Целью статьи является повышение активной безопасности группы МО в условиях плохой видимости на основе новых методов и средств информационной поддержки субъектов транспортного процесса.

Подходы: в качестве основного подхода к решению проблемы повышения активной безопасности мобильных объектов в условиях плохой видимости взято усовершенствование V2V-подхода для многостороннего обмена навигационной между МО и их позиционирования относительно оцифрованных границ ДП с использованием единого виртуального информационного пространства.

Результаты исследования: на основе V2V - подхода определяются отклонения от рекомендуемого коридора движения мобильных объектов с учетом геометрических характеристик дорожного полотна.

8. Хруль С.А. Адаптивный алгоритм обработки потока навигационных данных на основе метода диагностической фильтрации /Хруль С.А., Сонькин Д.М. // Известия Томского политехнического университета, №5. – 2012 [8].

Целью статьи является обработка потока навигационных данных для повышения достоверности и уменьшения объема исходных данных.

Подход: разработка адаптивного алгоритма отсева избыточных и ошибочных данных.

В результате исследования разработан адаптивный алгоритм отсева избыточных и ошибочных данных, работающий в режиме реального времени, основанный на диагностической фильтрации, позволяющий уменьшить поток навигационных данных, а также существенно снизить нагрузку на канал передачи данных.

9. Хруль С.А. Повышение точности позиционирования мобильных объектов на основе оригинальных методов фильтрации навигационных данных /Хруль С.А., Сонькин Д.М.// Интернет – журнал «Науковедение», №4. – 2013 [9].

Целью статьи является повышение точности позиционирования, которое можно достигнуть за счет применения различных алгоритмов обработки принимаемых навигационных данных.

Подходы: фильтрация ложных и избыточных данных полученных от GPS/ГЛОНАСС модуля, входящего в состав аппаратуры мобильного терминала.

В результате исследования разработан адаптивный метод отсева избыточных и ошибочных данных в режиме реального времени, основанный на диагностической фильтрации, позволяющий увеличить точность позиционирования, оптимизировать входной поток навигационных данных, а также существенно уменьшить нагрузку на канал передачи данных.

Результаты проведенного обзора публикаций по теме мониторинга мобильных объектов могут быть использованы для учебного процесса.

Список литературы

1. Аралбаев Т.З. Исследование погрешностей в системе мониторинга мобильных объектов на основе навигационного ключа /Аралбаев Т.З., Галимов Р.Р., Идрисов А.Ш., Каменева Е.В., Солдатов А.С.// Сборник статей XIII международной научно-практической конференции «Прогрессивные технологии в транспортных системах», 2017. – С. 9-12.

2. Григорьевский В.И. Мобильные приемо - передающие устройства для системы позиционирования в задачах контроля наземных объектов /В.И. Григорьевский// Измерительная техника, №5. - 2013. – С. 10-13.

3. Карпик А.П. Навигационно - информационная система точного позиционирования транспорта с использованием наземной инфраструктуры ГЛОНАСС /Карпик А.П., Ганагина И.Г., Косарев Н.С., Голдобин Д.Н.// Журнал «Гироскопия и навигация», №2. - 2015. – С. 47-57.

4. Каширская Е.П. Об алгоритме решения задачи определения координат текущего местоположения по телеметрической информации /Е.П. Каширская// Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника», №1. – 2014. – С. 106 – 109.

5. Сарайкин А. И. Позиционирование мобильного объекта на дорожном полотне в условиях дефицита информации /Сарайкин А. И., Аралбаев Т. З., Хасанов Р. И.// Вестник Оренбургского государственного университета, №4. - 2015. – С.114-118.

6. Хасанов Р. И. Инструментальная база для исследования режима позиционирования мобильного объекта в условиях дефицита информации /Хасанов Р. И., Сарайкин А. И., Аралбаев Т. З.// Журнал автомобильных инженеров, №1. - 2015. – С. 5-9.

7. Хасанов Р. И. Модифицированный «V2V» подход позиционирования мобильных объектов как средство снижения аварийности машин скорой помощи /Р. И. Хасанов// Альманах молодой науки, №2. - 2016. - С. 12 – 14 [7].

8. Хруль С.А. Адаптивный алгоритм обработки потока навигационных данных на основе метода диагностической фильтрации /Хруль С.А., Сонькин Д.М. // Известия Томского политехнического университета, №5. – 2012.

9. Хруль С.А. Повышение точности позиционирования мобильных объектов на основе оригинальных методов фильтрации навигационных данных /Хруль С.А., Сонькин Д.М.// Интернет – журнал «Науковедение», №4. – 2013.

НЕКОТОРЫЕ АСПЕКТЫ ВНЕДРЕНИЯ ИНТЕРАКТИВНЫХ МЕТОДОВ ОБУЧЕНИЯ БАКАЛАВРОВ НАПРАВЛЕНИЯ ПОДГОТОВКИ «МАТЕМАТИКА И КОМПЬЮТЕРНЫЕ НАУКИ»

Шакирова Д.У., канд. пед. наук, Усова Л.Б., канд. пед. наук
Оренбургский государственный университет

Современное производство формирует социальный заказ техническим вузам на подготовку высококомпетентных бакалавров, способных выполнять свои функции соответственно профилю направления подготовки на уровне мировых стандартов, готовых к постоянному профессиональному росту и мобильности. В связи с этим, система высшего образования предусматривает реализацию компетентностного подхода с использованием в учебном процессе интерактивных методов обучения.

Интерактивные методы способствуют введения в процесс обучения ситуаций реальной профессиональной деятельности, благодаря которым студенты решают различные задания, анализируют ситуации, что подтверждает одно из требований основных образовательных программ бакалавриата на основе федерального государственного образовательного стандарта (ФГОС).

В соответствии с ФГОС реализация учебного процесса предусматривает проведение различного рода занятий в интерактивных формах.

Основой высшего образования является фундаментальное образование, которое сводится к формированию системы профессиональных знаний, умений, навыков, способности логически рассуждать, анализировать, систематизировать факты, принимать решения и применять научный подход к изучению различных событий и процессов. В рамках ФГОС математическая подготовка является составной частью фундаментального образования бакалавров вуза.

Фундаментальность математической подготовки характеризуется многофункциональностью, наличием универсальных математических методов, способностью бакалавра на осуществление специализированной деятельности по рациональному использованию математического аппарата. Качество математического образования будущих бакалавров определяется интенсивностью реализации в процессе обучения интерактивных и информационно-коммуникативных технологий [6].

ФГОС высшего образования (ВО) по направлению подготовки «Математика и компьютерные науки» ориентирует вуз на конкретные виды профессиональной деятельности, к которым готовится выпускник, исходя из потребностей рынка. Объектами профессиональной деятельности будущих бакалавров направления подготовки «Математика и компьютерные науки» являются основные понятия фундаментальной (гипотезы, теоремы, методы, математические модели и др.) и прикладной (алгоритмы, программы, базы данных, операционные системы, компьютерные технологии и др.) математики. Данные объекты профессиональной деятельности являются составляющими в таких категориях общепрофессиональных компетенций ФГОС ВО как:

- *теоретические и практические основы профессиональной деятельности*: ОПК-4-способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем;

- *информационно-коммуникационные технологии для профессиональной деятельности:* ОПК-5-способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, в том числе отечественного производителя, и с учетом основных требований информационной безопасности [8].

Основной линией совершенствования подготовки студентов в современном вузе является внедрение интерактивных методов обучения, которое активизирует его как субъекта образовательной деятельности. Понятие интерактивные методы (в переводе с англ. *interaction* — взаимодействие, воздействие друг на друга) означает методы обучения, основанные на взаимодействии обучающихся между собой.

В своей работе, Гущин Ю.В. рассматривает понятие «интерактивное обучение» как:

– «обучение, построенное на взаимодействии учащегося с учебным окружением, учебной средой, которая служит областью осваиваемого опыта»;

– «обучение, которое основано на психологии человеческих взаимоотношений и взаимодействий»;

– «обучение, понимаемое как совместный процесс познания, где знание добывается в совместной деятельности через диалог».

Автор отмечает, что интерактивное обучение основано на собственном опыте обучающихся, а также на их прямом взаимодействии с областью осваиваемого профессионального опыта. При этом, обучение с использованием интерактивных технологий предполагает отличную от привычной логику образовательного процесса: не от теории к практике, а от формирования нового опыта к его теоретическому осмыслению через применение [3].

Как отмечает в своей работе Княжева В.В., согласно исследованиям, внедрение интерактивных форм обучения на занятиях можно рассматривать как одно из важнейших направлений в современном профессиональном образовании. Интерактивное обучение способствует эффективному вовлечению студентов в их активную познавательную деятельность, делает доступным и интересным учебный материал, подразумевает вполне конкретные и прогнозируемые цели, а также специальную подготовку преподавателя к занятиям. Подготовка к занятию предусматривает составление плана, методическую разработку занятия, отражающую четко поставленные цели, подготовку вопросов для обсуждения, проблемных ситуаций для коллективного обсуждения и решения, обдумывания организации деятельности каждого студента в условиях обучения, при которых студент чувствует свою успешность, интеллектуальную состоятельность, что делает продуктивным и успешным процесс обучения [5].

В своей работе, Болотюк Л.А. рассматривает три типа интерактивности в учебном процессе: взаимодействие студента и предмета обучения; взаимодействие студента и преподавателя; взаимодействие студентов.

В настоящее время в педагогике не существует единой классификации интерактивных методов обучения. Болотюк Л.А. приводит одну из классификаций интерактивных методов обучения:

1. Не имитационные, используемые в рамках традиционных форм учебной деятельности (проблемная лекция, лекция с разбором конкретных ситуаций, лекция с запланированными ошибками, лекция–визуализация, практические занятия, курсовое и дипломное проектирование и др.);

2. Имитационные, применение которых связано с использованием в учебном процессе новых методов обучения (игровые: деловые и ролевые игры, мозговой штурм, исследовательские игры, проектировочные игры; неигровые: дискуссия, тренинг, кейс-задания, метод развивающих операций, метод группового решения творческих задач и другие);

3. Вебинар, представленный в виде онлайн-обучения (беседа, лекция) в синхронном режиме, позволяющая в процессе обучения слушателям принимать активное участие посредством вопросов, выражения мнения, общения со всеми участниками [2].

Анализ научных исследований и педагогический опыт показывает, что обучающиеся бакалавриата направления подготовки «Математика и компьютерные науки» имеют разные по уровню знания по математике, причем чаще всего незначительные; у них, как правило, отсутствует интерес к ее изучению и очень низкая мотивация. В связи с этим, в процессе математической подготовки бакалавров для стимулирования их познавательной деятельности и личностного роста необходимо комплексное внедрение различных интерактивных методов обучения.

В процессе изучения математических дисциплин в рамках данного направления были внедрены те интерактивные методы, которые наиболее эффективны при создавшихся в вузе условиях и отвечают требованиям программ обучения. При этом учитывалась специфика общеобразовательных программ, учебных дисциплин, а также регламентации, предусмотренные образовательными стандартами. Приведем примеры интерактивных методов обучения, которые способствуют формированию соответствующих компетенций:

- лекция с запланированными ошибками (компетенцииУК-3,ОПК-1);
- учебные дискуссии (компетенции УК-3,УК-4,ОПК-1, ОПК-3);
- деловая игра (компетенции УК-1, ОПК-1, ОПК-4, ОПК-5);
- работа в малых группах (компетенции УК-1,УК-2,УК-6, ОПК-1,ОПК-4);
- кейс-метод (УК-1, УК-2, ОПК-1, ОПК-4, ОПК-5).

Представим примеры внедрения перечисленных выше интерактивных методов обучения при изучении математических дисциплин в рамках данного направления подготовки. В процессе изучения дисциплины «Дифференциальные уравнения» использовался один из наиболее распространённых интерактивных

методов обучения как *лекция с запланированными ошибками* на тему «Дифференциальные уравнения высших порядков». Такая форма организации лекции заинтересовывала внимание студентов на протяжении всего занятия, так как им предстояло найти ошибки. Особенно интересным получился результат, когда ошибки были дифференцированы по сложности и найти их удавалось не только сильным, хорошо подготовленным, но и слабым студентам.

Примером интерактивного метода обучения являлось *деловая игра*, которая применялась нами на занятии по дисциплине «Комплексный анализ» в конце изучения темы «Дифференцирование функций комплексного переменного». Данный метод позволил задействовать бакалавров в активную информационно-познавательную деятельность, в процессе которой они находили различные способы решения учебно-профессиональных задач с использованием программного пакета Mathcad, Excel. Деловая игра способствовала развитию познавательной активности бакалавров, творческому, операционному мышлению, повышению интереса к информационным технологиям как средству решения практико-ориентированных задач.

Самым распространенным интерактивным методом обучения является *учебная дискуссия*, которая была внедрена при изучении дисциплины «Дискретная математика, математическая логика и их приложения в информатике и компьютерных науках» на занятии по теме «Комбинаторика». Опыт проведения занятий в форме учебной дискуссии, позволил повысить интерес студентов к изучаемому материалу, способствовал расширению и углублению уже известной информации и ее систематизации, активизировать учебно-познавательную деятельность и обеспечить эффективность образовательного процесса.

Следующий *кейс-метод*, который мы использовали на практическом занятии по дисциплине «Дискретная математика, математическая логика и их приложения в информатике и компьютерных науках» на тему «Алгоритмы проверки формул Алгебры высказываний на тождественную истинность», характеризовался как метод анализа ситуаций. Использование данного метода обеспечивало не только прирост знаний, умений, навыков, способов деятельности и коммуникации, но и раскрытие новых возможностей студентов.

Работа в малых группах как пример интерактивного метода обучения нами осуществлялась в рамках лабораторной работы на тему «Метрические характеристики графа» по учебной дисциплине «Теория конечных графов». Данный метод способствует усилению процесса понимания, усвоения и творческого применения знаний при решении практических задач; повышению мотивации и вовлечению студентов в решение обсуждаемых задач.

Таким образом, практика внедрения интерактивных методов обучения обеспечивала развитие коммуникативных умений и навыков, активности в учебной деятельности; прочности знаний; самостоятельного поиска информации, что способствовало формированию необходимых компетенций и повышению качества подготовки будущих бакалавров.

Список литературы

1. Арсентьева, Е. С. Опыт применения интерактивных форм обучения в процессе преподавания технических дисциплин / Арсентьева Е. С., Косогова Ю. П., Мецлер А. А., Томилина М. Е. // Концепт. – 2016. – № 2 (февраль). – С. 81–85. – URL: http://e-koncept.ru/2016/16037.htm.

2. Болотюк, Л. А. Применение интерактивных методов обучения на практических занятиях по теории вероятностей и эконометрике / Л.А. Болотюк, А.М. Сокольникова, Е.А. Швед // Интернет-журнал Науковедение. 2013. №3 (16). URL: https://cyberleninka.ru/article/n/primenenie-interaktivnyh-metodov-obucheniya-na-prakticheskih-zanyatiyah-po-teorii-veroyatnostey-i-ekonometrike.

3. Гущин, Ю.В. Интерактивные методы обучения в высшей школе. / Ю.В. Гущин - Психологический журнал Международного университета природы, общества и человека Дубна № 2, 2012. - Режим доступа: http://www.psyanima.ru.

4. Двуличанская, Н.Н. Интерактивные методы обучения как средство формирования ключевых компетенций / Н.Н. Двуличанская Н.Н. – Наука и образование. - апрель 2011. – Режим доступа: http://technomag.edu.ru/doc/172651.html

5. Княжева, В.В. Теория и практика внедрения интерактивных форм обучения на уроках общественных дисциплин в профессиональном образовании /В.В. Княжева. - «Молодой учёный» . № 21 (101) . Ноябрь, 2015 г.- С. 784-787.

6. Ольховая, Т.А. Информационно-познавательная самостоятельность как фактор становления субъектной позиции студентов бакалавриата / Т.А., Ольховая, Д.У. Шакирова // Современные проблемы науки и образования. – 2014. – № 5.; URL: http://science-education.ru/ru/article/view?id=14685.

7. Спирина, М.Л. Использование технологий интерактивного обучения в подготовке бакалавров психолого-педагогического образования / М.Л. Спирина - Историческая и социально-образовательная мысль. 2014. № 4 (26).

8. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки (уровень бакалавриата) Режим доступа: http://www.osu.ru/docs/fgos/vo3++/02.03.01 _Math_i_komp_nauki.pdf.

ИСПОЛЬЗОВАНИЕ UML-ДИАГРАММ КЛАССОВ ДЛЯ ПОСТРОЕНИЯ ОБЪЕКТНЫХ МОДЕЛЕЙ ДАННЫХ ЭКОНОМИЧЕСКИХ ПРИЛОЖЕНИЙ НА ПЛАТФОРМЕ «1С:ПРЕДПРИЯТИЕ»

Широбокова С.Н., канд. экон. наук, Сериков О.Н.
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, г. Новочеркасск

По предложенной в [1-2] методике построение модели прикладных объектов предлагается реализовывать с помощью диаграммы классов унифицированного языка моделирования *UML*. Рассмотрим подробнее аспекты использования диаграмм этого типа в проектной практике для отражения структуры и взаимосвязей прикладных объектов конфигураций.

Принадлежность прикладного объекта к тому или иному прототипу отражается с помощью *стереотипов* класса (<<справочник>>, <<отчет>>, <<документ>> и проч.). Стереотипы обеспечивают классификацию прикладных объектов на уровне объектной модели по принадлежности к предопределенным платформой прототипам [1]. Во второй секции описываются реквизиты объекта. В третьей секции класса могут быть указаны экспортные процедуры, описанные в модуле объекта, и стандартные обработчики (например, *ПередЗаписью*() и др.), если разработчик определяет их для объекта.

В обозначениях классов на *UML* диаграмме может присутствовать четвертая секция для указания семантической информации справочного характера. Например, для решений на платформе «1С:Предприятие» рекомендуется в этой секции отражать настройку некоторых свойств объектов, от которых во многом зависит функциональность объекта [2]. Для справочников – это иерархичность, для плана счетов – признаки учета, признаки учета субконто, для регистра бухгалтерии – используемый план счетов, для плана видов расчета – использование периода действия, зависимость от базы, перечень базовых планов видов расчета, для регистра расчета – используемый план видов расчета, использование периода действия, периодичность и др. На рис. 1 четвертая секция использована, например, для отражения вида регистра – для регистров накопления, периодичности и режима записи – для регистров сведений.

Согласно методике [1] применительно к моделям приложений на платформе «1С:Предприятие» рекомендуется применение нотаций типов отношений, описанное ниже:

– *отношение обобщения* – для отражения наследования предопределенных атрибутов и процедур прототипа конкретными прикладными объектами;

– *отношение зависимости* может быть использовано в нескольких случаях, например:

- для отражения взаимосвязи между прикладными объектами, когда один объект использует значения атрибутов другого объекта в своих процедурах;

- для отражения взаимосвязи отчета с теми объектами, из которых запросами извлекается необходимая для его формирования информация (рис. 1);
- для отражения взаимосвязи между регистром и документом, выполняющим движения в регистре;

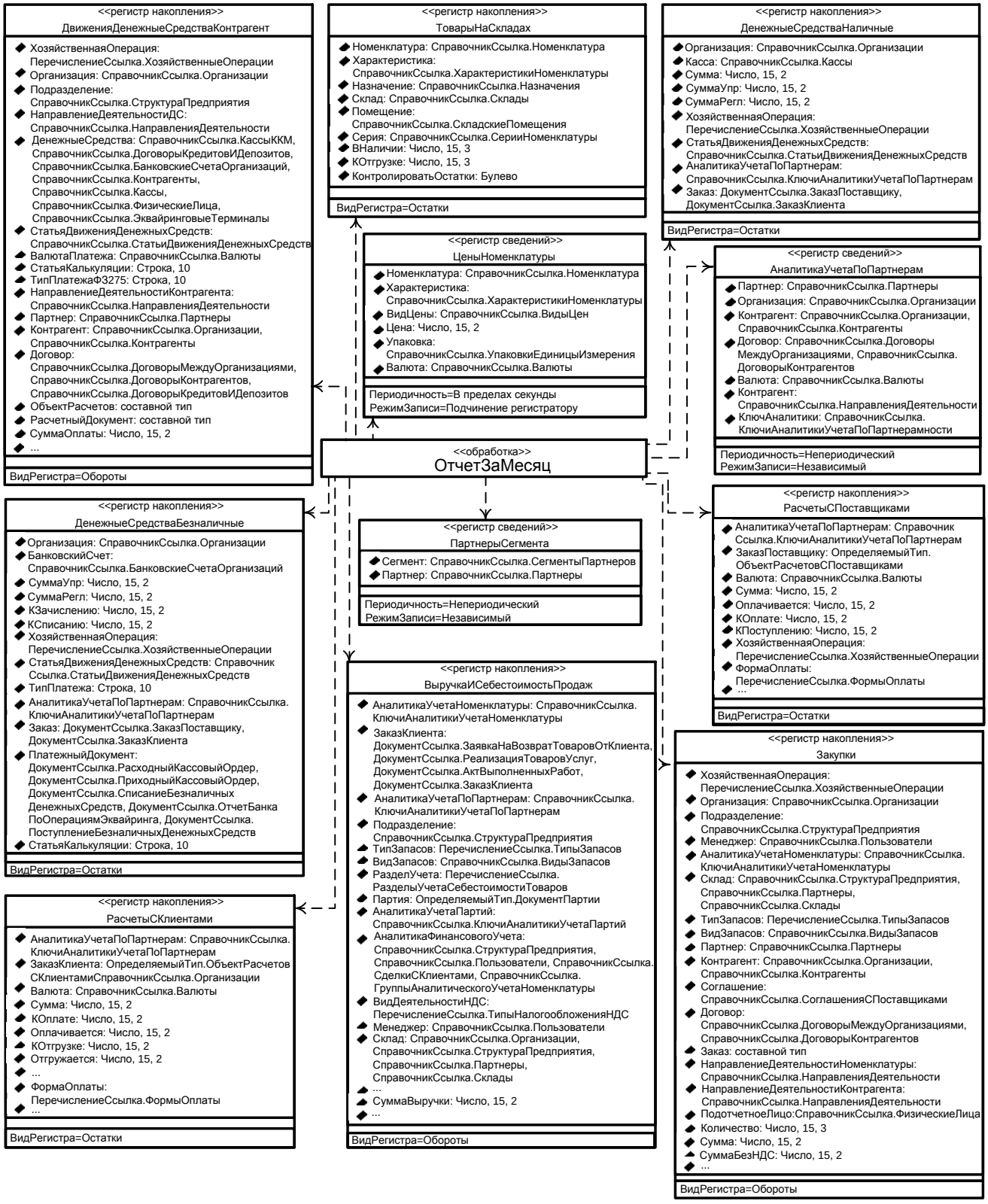


Рисунок 1 – Примеры описания реквизитов и свойств справочников, регистров сведений, регистров накопления

– *отношение ассоциации* используется для описания структурных связей между объектами на диаграмме классов, возникающих в случае наличия в структуре объектов реквизитов ссылочного типа (рис. 2);

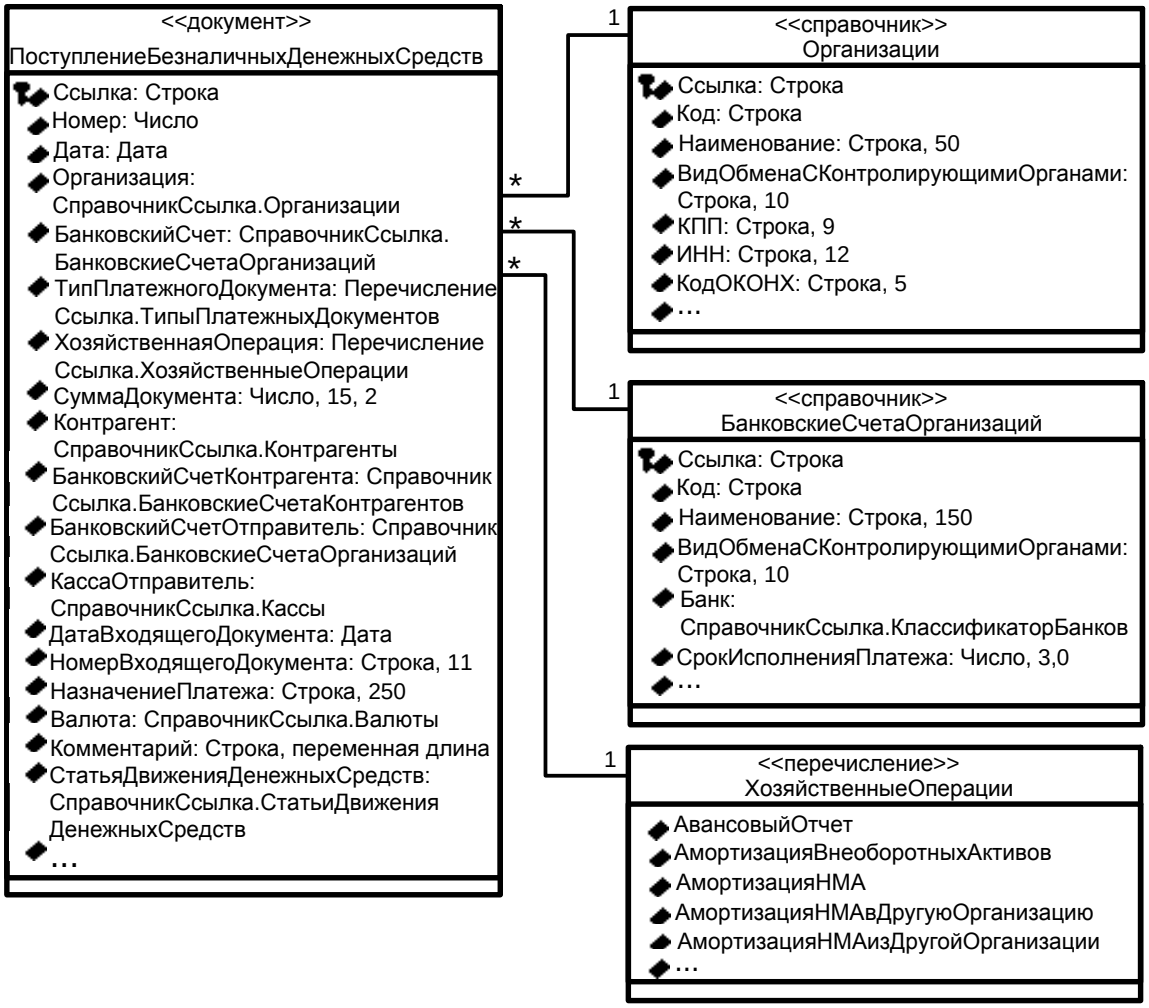


Рисунок 2 – Примеры использования отношений ассоциации для отражения связей между объектами при наличии реквизитов ссылочного типа

– *отношение агрегации* применимо для описания системных взаимосвязей типа «часть-целое» между прикладными объектами (например, между справочником-владельцем и подчиненным справочником) – рис. 3;

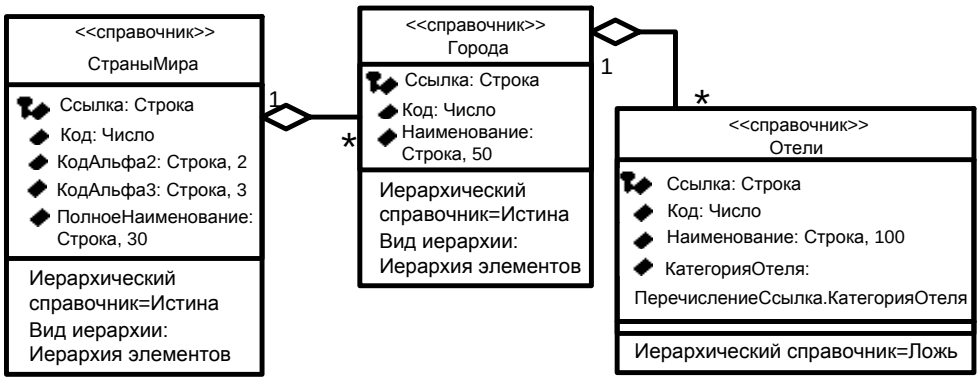


Рисунок 3 – Примеры использования отношений агрегации

– *исключающая ассоциация* может быть использована для отражения составного типа данных реквизита объекта, включающего ссылочные типы (рис. 4);

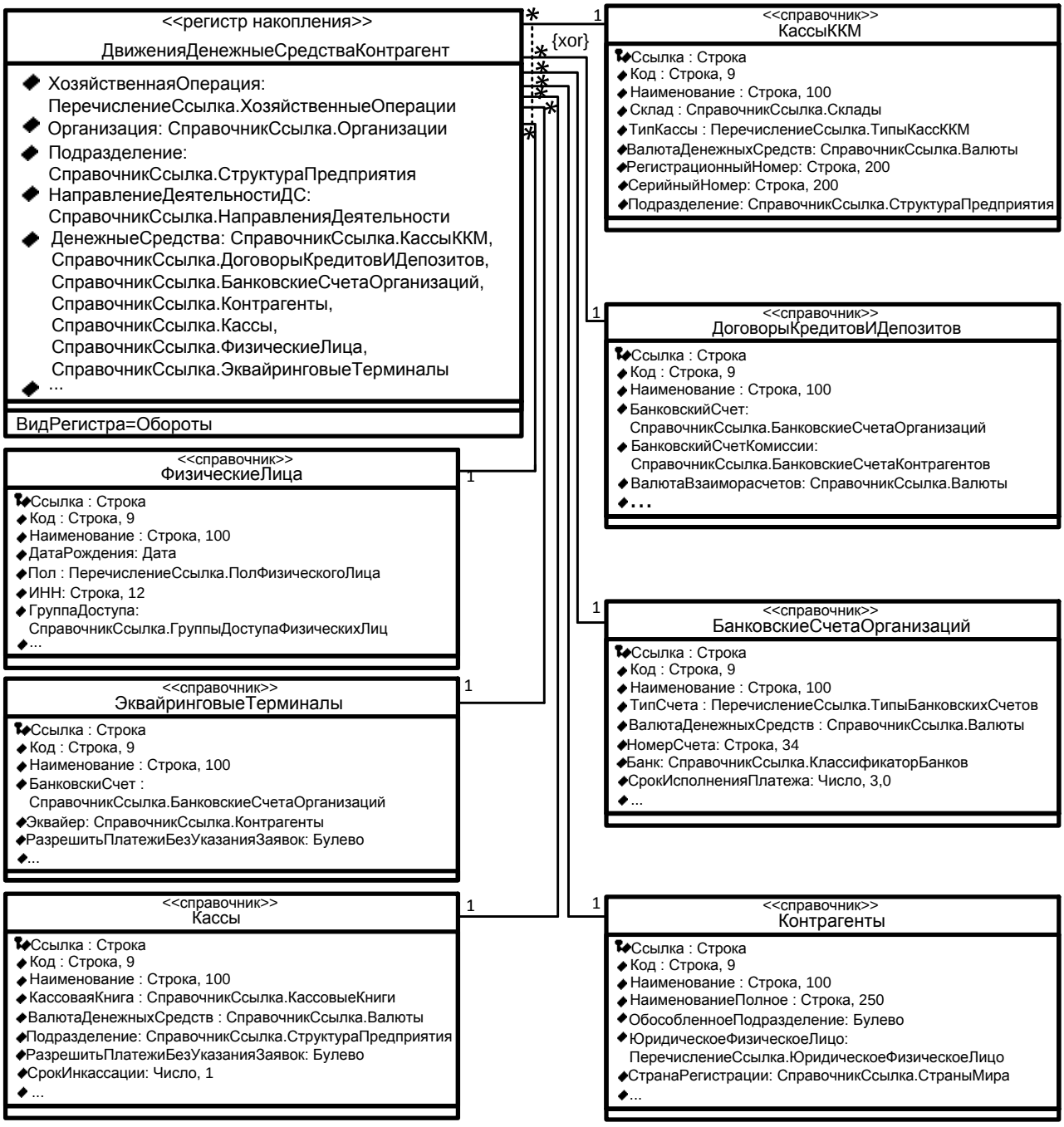


Рисунок 4 – Отношение «Исключающая ассоциация»

– *отношение композиции* может быть использовано для описания составной структуры сложного прикладного объекта (например, справочника или документа), включающего подчиненную табличную часть (рис. 5).

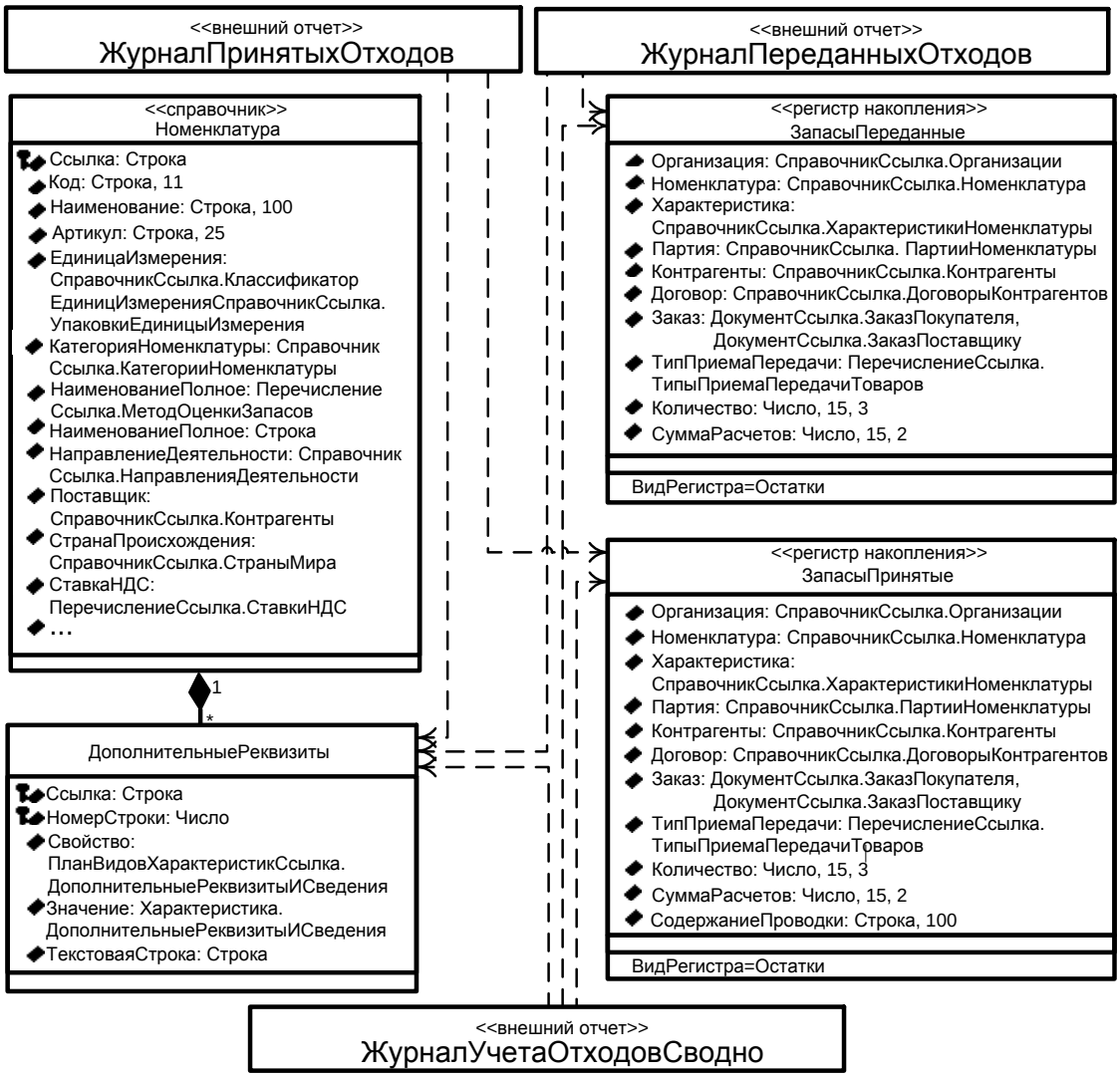


Рисунок 5 – Пример отношения композиции и отношения зависимости

Методика позволяет разработать формализованную *UML*-модель конфигурации как основу для дальнейшей программной реализации приложений. Апробированная в течение нескольких лет в рамках курсовых и выпускных квалификационных работ студентов методика также может быть использована в проектной деятельности компаний, занимающихся внедрением типовых конфигураций на платформе «1С:Предприятие», для документирования аспектов доработки типовых решений под требования пользователя.

Список литературы

1. Широбокова С.Н. Методика построения объектно-ориентированных моделей экономических приложений на платформе "1С:Предприятие" с использованием языка UML // Вестник Юж.-Рос. гос. техн. ун-та (Новочерк. политехн. ин-та). Сер. Соц.-экон. науки.– 2014.– № 2.– С. 28-33.

2. Широбокова С.Н. Аспекты методики UML-моделирования предметно-ориентированных экономических информационных систем на платформе "1С:Предприятие" // Перспективы науки.– 2015.– №10.– С. 119-125.