**МЕТОДИКА**

**проведения Научно-исследовательского семинара**

**«Верификация моделей программ»**

**Введение**

Программа развития Государственного университета - Высшей школы экономики, в отношении которого установлена категория "национальный исследовательский университет", утверждена приказом Минобрнауки России от 26 ноября 2009 года № 677. В рамках Программы развития предусматривается вовлечение студентов всех факультетов и отделений университета в научно-исследовательскую деятельность, начиная с первого года обучения. Такой подход начал реализовываться на отделении программной инженерии с начала 2010-2011 учебного года и нашел отражение в учебной программе первого курса бакалавриата.

Научно-исследовательские семинары для 1-го курса студентов бакалавриата проводились впервые в 2010-2011 учебном году. Данная методика описывает подход к проведению научно-исследовательского семинара со студентами 1-го курса бакалавриата на отделении Программной инженерии факультета Бизнес-информатики по одному из трех тематических направлений, предлагавшихся в 2010-2011 учебном году студентам 1-го курса бакалавриата отделения Программной инженерии, начиная с первых дней обучения. Студентам были предложены три научно-исследовательских семинара, тематика которых указана ниже:

* верификация моделей программ;
* ресурсно-эффективные комбинированные алгоритмы;
* компонентно-ориентированное программирование.

Выбор этих направлений (тем) для семинаров продиктован следующими соображениями:

* тематика научного семинара первого курса не должна дублировать и/или опережать изучение предметов и тем, преподаваемых в рамках учебной программы;
* тематика семинаров должна способствовать более глубокому пониманию изучаемых по программе предметов, отражая современные подходы к использованию научных результатов в данной области;
* тематика семинаров должна стимулировать развитие интереса к самостоятельным исследованиям и разработкам студентов;
* тематика должна соответствовать научным интересам руководителей семинаров, способных заинтересовать участников семинаров и привлечь их к исследованиям на современном уровне;
* спектр предлагаемых направлений должен быть достаточно широк для возможностей адаптации к различным уровням подготовки участников, еще не прошедших фундаментального курса подготовки;
* спектр предлагаемых направлений должен давать студентам возможность выбора направлений исследований с учетом их пристрастий и интересов в рамках общего направления – программной инжененрии (Computer Science vs. Software Engineering), которое, как следует из названия, является разновидностью инженерной деятельности, предусматривающей создание, в конечном счете, работающих программных продуктов.

Предполагалось, что участие каждого студента в одном из семинаров является обязательным. В целях ориентации студентов на начальном этапе приветствовалось посещение ими более одного семинара с тем, чтобы позволить им сделать осознанный выбор направления работы. С этой же целью первый семинар содержал краткие презентации направлений исследований по всем предложенным темам.

Последующая практика показала, что многим студентам 1-го курса бакалавриата сложно сделать самостоятельный выбор направления исследований – либо по причине резкой смены обстановки в целом по сравнению со школьными навыками (для менее подготовленной к исследовательской деятельности части слушателей), либо по причине наличия интереса к более чем одной теме из числа предложенных (для более продвинутых слушателей). Тем не менее, один из семинаров должен был быть выбран каждым студентом в качестве основного, участие в котором обязательно в соответствии с учебным планом. Решение было найдено путем сочетания участия студентов в научно-исследовательских семинарах с их деятельностью по курсовым работам: обязательным для участия студента был принят научно-исследовательский семинар, тематика которого в большей степени соответствует выбранной (в это же время) и утвержденной теме курсовой работы. Такое разделение студентов по предложенным направлениям семинаров не является, однако, препятствием для участия студентов в работе других семинаров, но способствует, как представляется, более качественному выполнению курсовых работ, обязательная защита которых проводится в конце каждого учебного года.

Далее в данной Методике рассматриваются вопросы, относящиеся к проведению научно-исследовательского семинара по направлению «Верификация моделей программ» в 2010-2011 учебном году.

**1. Основные задачи научно-исследовательского семинара.**

Тематика семинара «Верификация моделей программ» связана с фундаментальной проблемой разработки средств и методов повышения надежности программ и программных систем и снижения затрат при их разработке.

В последние десятилетия резко выросло число и сложность окружающих нас программных и программно-аппаратных систем, что привело не только к росту уровня жизни, но и к росту риска сбоев, катастроф и кризисов, вызванных ошибками разработки и/или управления такими системами. Можно сказать, что сложность разрабатываемого программного обеспечения подошла к границе его понимания. Так, например, операционная система Microsoft Windows XP содержит 40 миллионов строк. Поэтому понятно, что ошибки в сложных программных системах не являются чем-то исключительным. На форуме старейшей и наиболее крупной международной организации в компьютерной области Ассоциации вычислительной техники ACM (<http://catless.ncl.ac.uk/Risks/>) собрана информация о тысячах случаев отказа техники по причине ошибок, допущенных разработчиками программного и программно-аппаратного обеспечения. Такие отказы приводят как к большим убыткам, так и к невосполнимым потерям.

Задача верификации (проверки правильности) программ состоит в проверке соответствия программы ее спецификации. Впервые эта задача была поставлена Р. Флойдом и Э. Хоаром в начале 70-х годов прошлого века. В настоящее время теории и технике верификации посвящено огромное количество литературы от научных статей и монографий до университетских курсов. В то же время, верификация программ и программных систем остается и в настоящее время одним из наиболее бурно развивающихся научных направлений в области программной инженерии. В 2007 году премия Тьюринга ассоциации ACM (аналог Нобелевской премии в области компьютерных наук) была присуждена Э. Кларку, Э. Эмерсону и Дж. Сифакису за их вклад в доведение метода верификации *model checking* до производственной технологии, позволяющей осуществлять верификацию моделей реальных программных и программно-аппаратных систем.

Таким образом, тематика семинара «Верификация моделей программ» связана с актуальной научной проблемой, важность которой можно и нужно объяснять студентам уже на первом курсе. Студенты должны понимать, что разработка программного обеспечения – это не просто создание программного кода, который «работает», но и обоснование корректности разработанной программы.

Важной особенностью исследований, связанных с верификацией программ, является широкое использование формальных математических моделей программ и методов теоретической информатики для решения насущных практических проблем разработки и сопровождения программного обеспечения. Знакомство студентов 1 курса с этой областью исследований показывает им важность изучения фундаментальных основ математической логики и дискретной математики, тесную связь между такими курсами учебного плана, как «Математическая логика и теория алгоритмов», «Дискретная математика» и курсом «Программирование».

Верификация моделей программ – достаточно сложная, обширная и быстро развивающаяся, современная область информатики. Вместе с тем, в этой области можно выделить разделы, не требующие специальных предварительных знаний. Вопросы, связанные с частичной и тотальной корректностью последовательных программ, можно обсуждать уже со студентами первого курса. Более того, изучение методов верификации на примере совсем небольших и простых программ оказывается очень полезным и с точки зрения выработки у студентов навыков программирования в «хорошем стиле». Методология разработки программы одновременно с доказательством ее корректности была разработана Н. Виртом в 70-х годах прошлого века, и работы Н. Вирта оказали значительное влияние на дальнейшее развитие программирования. Поэтому семинар «Верификация моделей программ» является полезным для студентов дополнением к базовому курсу «Программирование».

Особенно подвержены ошибкам параллельные, распределенные и сетевые программы, доля которых в общем объеме программного обеспечения постоянно возрастает. Хорошо известно, что даже в тех случаях, когда функционирование каждого из параллельных взаимодействующих компонентов системы представляется простым и понятным, человеку трудно понять поведение системы в целом из-за взаимозависимости компонентов. Л. Лэмпорт, известный специалист в области распределенных алгоритмов, пишет: «Параллельные системы, которые работают правильно “почти всегда”, годами могут сохранять тонкие ошибки, проявляющиеся в редких, исключительных ситуациях. Такие ошибки практически невозможно обнаружить тестированием».

Сложность распределенных систем связана не с собственно вычислениями, а с управлением взаимодействиями между процессами. Поэтому при анализе распределенной программной системы можно абстрагироваться от вычислений и рассматривать формальную модель системы с точки зрения управления взаимодействием процессов. В настоящее время разработано большое число формализмов для моделирования и анализа распределенных и параллельных систем. Среди наиболее популярных таких формализмов – сети Петри. Сети Петри – простой и наглядный формализм. Другое достоинство сетей Петри – хорошо разработанные теория и методы анализа поведенческих свойств. Основы сетей Петри можно читать уже студентами первого курса. Опыт проведения семинара в 2010-11 учебном году показывает, что задачи моделирования различных динамических систем сетями Петри вызывают у студентов большой интерес. Важно также, что любая задача на моделирование реальное системы – это небольшое исследование.

Таким образом, научно-исследовательский семинар «Верификация моделей программ» позволит вырабатывать у студентов компетенции и навыки, связанные с научно-исследовательской работой.

В частности, в результате участия в научном семинаре студенты смогут приобрести следующие компетенции:

по общей методологии научного исследования:

* овладеть базовыми умениями и навыками ведения самостоятельных исследований на примере верификации программ и программных систем;
* получить навыки выступлений с научными докладами, оформления содержательных презентаций
* научится корректно вести научные дискуссии;
* научиться работать с научной литературой, в том числе, с литературой на английском языке;

по тематике научного семинара:

* иметь представление о современных методах и возможностях обеспечения надежности программ и программных систем;
* получить углубленные знания в области средств и методов формальной спецификации и верификации программ;
* познакомиться с формализмами для моделирования параллельных и распределенных систем;
* получить навыки структурного анализа формальных моделей параллельных и распределенных систем;
* освоить методы работы с конкретными верификационными системами;
* приобрести практические навыки экспериментального построения моделей программных систем и исследования их корректности.

**2. Порядок организации семинара**

Научно-исследовательский семинар (НИС) проводится в течение 1-4 модулей первого года обучения бакалавров по направлению «Программная инженерия». На протяжении всего этого периода он включает еженедельные аудиторные занятия по утвержденному расписанию и самостоятельную работу студентов. Продолжительность семинара составляет 72 аудиторных учебных часа в форме практических занятий и 36 часов самостоятельной работы. Рубежный контроль – зачет в конце четвертого модуля. Количество кредитов – 3.

Часы НИС учитываются в учебной нагрузке преподавателей, проводящих занятия в соответствии с порядком, установленным в НИУ ВШЭ.

Научно-исследовательский семинар «Верификация моделей программ» организуется кафедрой управления разработкой программного обеспечения отделения программной инженерии факультета бизнес-информатики.

Работа в научно-исследовательском семинаре является для студента обязательной. Каждый студент первого курса выбирает в качестве обязательного один из трех предлагаемых семинаров. При этом студент вправе посещать другие научно-исследовательские семинары, организованные отделением программной инженерии для студентов 1 курса, на добровольной основе без обязательств по сдаче зачетов.

**3. Формы работы на семинаре**

При проведении научно-исследовательского семинара используются следующие формы работы:

* лекции преподавателя и приглашенных докладчиков;
* обсуждение и совместное решение задач;
* доклады и сообщения студентов;
* представление студентами собственных примеров и решений;
* демонстрация программных средств для моделирования и верификации программных систем.

Научно-исследовательский семинар направлен на выработку у студентов таких навыков, как:

* восприятие и критический анализ нового материала;
* понимание взаимосвязей между различными предметами, изучаемыми студентами на 1 курсе бакалавриата;
* презентации научных сообщений;
* умение формулировать вопросы и задачи;
* культура ведения научных дискуссий.

Поэтому все формы работы предусматривают режим свободной дискуссии: возможность задать вопрос по ходу лекции или сообщения, генерирование идей, предложение альтернативных решений, обсуждение как содержания, так и формы представления материала.

**4. План работы по модулям**

***В первом модуле*** проводятся лекции руководителей всех научных семинаров для студентов 1 курса отделения программной инженерии. На этих лекциях студенты знакомятся с порядком организации и проведения научно-исследовательских семинаров, тематикой семинаров, с методами и особенностями проведения научных исследований. Каждый руководитель представляет проблемную область, связанную с темой семинара, актуальность и прикладное значение тематики семинара.

В рамках представления научно-исследовательского семинара «Верификация моделей программ» со студентами обсуждаются, в частности, следующие вопросы:

* Что такое корректная программа?
* Можно ли избежать ошибок в программах?
* Цена ошибки в программе.
* Тестирование: достоинства и недостатки.
* Формальная спецификация: для чего это нужно?
* Верификация и валидация программ.
* Верификация vs. тестирование.
* Верификация: пределы и возможности.

В конце первого модуля каждый студент выбирает один из предложенных научных семинаров в качестве обязательного.

***Во втором модуле*** занятия семинара посвящены основам верификации последовательных программ. В частности, рассматриваются и обсуждаются следующие вопросы:

* Что такое формальный язык? Как записать утверждение о корректности программы?
* Перевод с естественного языка на формаоьный.
* Утверждения о частичной и тотальной корректности программ.
* Можно ли доказать корректность программы?
* Доказательства и правдоподобные рассуждения. Ошибки в доказательствах.
* Метод Флойда проверки частичной корректности программ.
* Циклы и инварианты циклов.
* Можно ли доказать, что программа останавливается?

***В третьем модуле*** на семинаре рассматриваются вопросы моделирования и анализа поведенческих свойств параллельных и распределенных систем. В частности, рассматриваются и обсуждаются следующие вопросы:

* Зачем нужны формальные модели?
* Что мы моделируем?
* Основные управляющие конструкции параллельных и распределенных систем.
* Сети Петри и моделирование распределенных систем.
* Структура сети Петри и ее поведение.
* Поведенческие свойства: что нужно проверять?
* Свойства безопасности и свойства живости.
* Раскрашенные сети Петри.

***В четвертом модуле*** студенты готовят зачетные задания и курсовые работы по тематике семинара. В это время семинар работает в режиме консультаций. Студенты готовят доклады и презентации на итоговую конференцию.

**5. Схема организации семинара**

Общая схема организации НИС представлена в таблице. Реализация отдельных форм не обязательно полностью совпадает с границами соответствующих модулей, однако приоритет в каждом модуле отдается именно указанным формам.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **I курс бакалавриата** | **Модули** | | | |
| **I** | **II** | **III** | **IV** |
|  | Введение в тематику семинара. Выбор студентами научного семинара, который будет для них обязательным. | Основные понятия верификации последовательных программ | Модели параллельных и распределенных систем. Сети Петри. Анализ поведенческих свойств сетей Петри. | Выполнение зачетного задания и его оформление в виде презентации.  Проведение мини-конференции. |
| Формы НИС | Лекции руководителей семинаров и приглашенных исследователей по тематике объявленных научных семинаров. Обсуждения состояния дел в области верификации программ и программно-аппаратных систем с участниками семинара | Лекции руководителя семинара и приглашенных исследователей.  Обсуждение и совместное решение задач.  Презентации сообщений и докладов участников семинара. | Лекции руководителя семинара и приглашенных исследователей.  Обсуждение и совместное решение задач.  Презентации сообщений и докладов участников семинара.  Презентации программных средств для моделирования и анализа сетей Петри. | Обсуждение форм и приемов преставления научного сообщения.  Выступления участников семинара по результатам проведенных мини-исследований. |

**Список участников семинара в 2010-11 учебном году:**

|  |  |
| --- | --- |
| **1** | Авхадеев Булат Ринатович |
| **2** | Евсеев Игорь Андреевич |
| **3** | Ким Ок Дя |
| **4** | Кирилов Алексей Сергеевич |
| **5** | Клюева Дарья Сергеевна |
| **6** | Ковалева Екатерина Викторовна |
| **7** | Коновалов Тимур Александрович |
| **8** | Кошкин Андрей Андреевич |
| **9** | Курамшин Ринат Анвярович |
| **10** | Курненкова Ирина Алексеевна |
| **11** | Мельников Илья Андреевич |
| **12** | Никаноров Александр Андреевич |
| **13** | Рацеров Андрей Николаевич |
| **14** | Рашидов Дамир Раушанович |
| **15** | Сивакова Анна Николаевна |
| **16** | Сныткин Максим Алексеевич |
| **17** | Солдатенко Мария Александровна |
| **18** | Сотов Александр Николаевич |
| **19** | Сысоев Герман Геннадьевич |
| **20** | Тимеркаева Анна Маратовна |
| **21** | Сергеев Владимир Дмитриевич |
| **22** | Фрумин Даниил Исакович |
| **23** | Хатту Павел Андреевич |
| **24** | Цвигун Евгения Викторовна |
| **25** | Шилов Артём Владимирович |
| **26** | Яхиев Иса Джабраилович |

**6. Промежуточная отчетность студентов по семинару**

В качестве *рубежного контроля* предусматривается зачет по итогам года. Задолженность по научно-исследовательскому семинару приравнивается к обычной академической задолженности.

*Текущий контроль* включает учет посещаемости научного семинара и оценку качества подготовки и активности участников семинара: доклады, презентации, оппонирование, критические выступления, решение задач и реализация компьютерных программ.

Зачет в конце 4 модуля проходит в форме научной конференции. Каждый участник семинара представляет решение некоторой задачи по тематике семинара. Задача представляет собой небольшое исследование, включающее построение формальной модели программы или системы и характеризацию ее поведенческих свойств. Студент готовит презентацию доклада. Каждый доклад сопровождается обсуждением: студенты задают вопросы докладчику, обсуждают достоинства и недостатки предложенного решения, альтернативные подходы к решению представленной задачи.

*Пример зачетной задачи:*

Построить формальную модель динамической системы по выбору (железнодорожный переезд, регулируемый светофорами перекресток, локальная сеть с общим принтером, компьютерная игра, интерактивный алгоритм, кофейный автомат и т.п.) в виде обыкновенной или раскрашенной сети Петри. Указать, какие из управляющих конструкций (последовательное выполнение, недетерминированный выбор, последовательное выполнение) используются в этой модели. Описать свойства, которым должно удовлетворять поведение модели.

**7. Руководство семинаром**

Руководитель семинара – профессор кафедры управления разработкой программного обеспечения отделения программной инженерии д.ф.-м.н., профессор И.А. Ломазова.

**8. Список литературы**

1. Карпов Ю.Г. MODEL CHECKING. Верификация параллельных и распределенных программ и систем. – СПб.: БХВ-Петербург, 2010. – 560 с.
2. Ben-Ari M. Principles of the Spin Model Checker. – Springer-Verlag, 2008. – 216 p. (доступна через электронную библиотеку ГУ ВШЭ)
3. Ломазова И.А. Сети Петри и анализ поведенческих свойств распределенных систем. – Ярославль: ЯрГУ, 2002. 164 с.
4. Миронов А.М. Теория процессов. М.: МГУ. Доступна на <http://intsys.msu.ru/staff/mironov/processes.pdf>.
5. Грис Д. Наука программирования. – М.: Мир, 1984. – 416 с.
6. Хопкрофт Дж., Мотвани Р., Ульман Дж. Введение в теорию автоматов, языков и вычислений: Пер. с англ. М.: Издательский дом "Вильямс", 2008. – 528 c.: ил.
7. Новиков Ф.А. Дискретная математика для программистов – СПб.: Питер 2008. – 304 с.: ил.
8. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking. – М.: МЦНМО, 2002. – 416 с.
9. Joseph Sifakis. A vision for computer science – the system perspective. Cent. Eur. J. Comp. Sci., 1(1), 2011. 108-116