МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Самарский государственный технический университет»
(ФГБОУ ВПО «СамГТУ»)

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ДИСЦИПЛИНЕ «МОДЕЛИ И АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Самара 2014г.

Саушкин М.Н.,

Методические указания по дисциплине «Модели и алгоритмы защиты информации» / Самар. гос. техн. ун-т; Сост. *Саушкин М.Н.* Самара, 2014г.

Методические указания предназначены для работы в аудитории и самостоятельной работы магистров по направлению подготовки 01.04.02 (010400.68) «Прикладная математика и информатика».

Печатается по решению методического совета Инженерно-экономического факультета

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Магистр по направлению подготовки 010400 Прикладная математика и информатика в соответствии с выбранными приоритетными видами профессиональной деятельности должен быть подготовлен к решению следующих профессиональных задач:

в научной и научно-исследовательской деятельности:

– изучение новых научных результатов, научной литературы или научно-исследовательских проектов в соответствии с профилем объекта профессиональной деятельности;

– применение наукоемких технологий и пакетов программ для решения прикладных задач в области физики, химии, биологии, экономики, медицины, экологии; изучение информационных систем методами математического прогнозирования и системного анализа;

– изучение больших систем современными методами высокопроизводительных вычислительных технологий, применение современных суперкомпьютеров в проводимых исследованиях;

– исследование и разработка математических моделей, алгоритмов, методов, программного обеспечения, инструментальных средств по тематике проводимых научно-исследовательских проектов;

– составление научных обзоров, рефератов и библиографии по тематике проводимых исследований;

– участие в работе научных семинаров, научно-тематических конференций, симпозиумов;

– подготовка научных и научно-технических публикаций;

в проектной и производственно-технологической деятельности:

– исследование математических методов моделирования информационных и имитационных моделей по тематике выполняемых научно-исследовательских прикладных задач или опытно-конструкторских работ;

– исследование автоматизированных систем и средств обработки информации, средств администрирования и методов управления безопасностью компьютерных сетей;

– изучение элементов проектирования сверхбольших интегральных схем, моделирование и разработка математического обеспечения оптических или квантовых элементов для компьютеров нового поколения;

– разработка программного и информационного обеспечения компьютерных сетей, автоматизированных систем вычислительных комплексов, сервисов, операционных систем и распределенных баз данных;

– разработка и исследование алгоритмов, вычислительных моделей и моделей данных для реализации элементов новых (или известных) сервисов систем информационных технологий;

– разработка архитектуры, алгоритмических и программных решений системного и изучение языков программирования, алгоритмов, библиотек и пакетов программ, прикладного программного обеспечения;

– продуктов системного и прикладного программного обеспечения;

– изучение и разработка систем цифровой обработки изображений, средств компьютерной графики, мультимедиа и автоматизированного проектирования;

– развитие и использование инструментальных средств, автоматизированных систем в научной и практической деятельности;

в педагогической деятельности:

– владение методикой преподавания учебных дисциплин;

– владение методами электронного обучения;

– консультирование по выполнению курсовых и дипломных работ студентов образовательных учреждений высшего профессионального и среднего профессионального образования по тематике в области прикладной математики и информационных технологий;

– проведение семинарских и практических занятий по общематематическим дисциплинам, а также лекционных занятий по профилю специализации.

Выпускник должен обладать следующими общекультурными компетенциями:

– способностью понимать философские концепции естествознания, владеть основами методологии научного познания при изучении различных уровней организации материи, пространства и времени (ОК-1);

– способностью иметь представление о современном состоянии и проблемах прикладной математики и информатики, истории и методологии их развития (ОК-2);

– способностью использовать углубленные теоретические и практические знания в области прикладной математики и информатики (ОК-3);

– способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение (ОК-4);

– способностью порождать новые идеи и демонстрировать навыки самостоятельной научно- исследовательской работы и работы в научном коллективе (ОК-5);

– способностью совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности (ОК-6);

– способностью и готовностью к активному общению в научной, производственной и социально-общественной сферах деятельности (ОК-7);

– способностью свободно пользоваться русским и иностранным языками как средством делового общения; способность к активной социальной мобильности (ОК-8);

– способностью использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов (ОК-9).

Выпускник должен обладать следующими профессиональными компетенциями:

– способностью проводить научные исследования и получать новые научные и прикладные результаты (ПК-1);

– способностью разрабатывать концептуальные и теоретические модели решаемых научных проблем и задач (ПК-2);

– проектная и производственно-технологическая деятельность: способностью углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности (ПК-3);

– способностью разрабатывать и оптимизировать бизнес-планы научно-прикладных проектов (ПК-4);

– организационно-управленческая деятельность: способностью управлять проектами (подпроектами), планировать научно-исследовательскую деятельность, анализировать риски, управлять командой проекта (ПК-5);

– способностью организовывать процессы корпоративного обучения на основе технологий электронного и мобильного обучения и развития корпоративных баз знаний (ПК-6);

– нормативно-методическая деятельность: способностью разрабатывать и оптимизировать бизнес-планы научно-прикладных проектов (ПК-7);

– педагогическая деятельность: способностью проводить семинарские и практические занятия с обучающимися, а также лекционные занятия спецкурсов по профилю специализации (ПК-8);

– способностью разрабатывать учебно-методические комплексы для электронного и мобильного обучения (ПК-9);

– способностью разрабатывать аналитические обзоры состояния области прикладной математики и информационных технологий по профильной направленности ООП магистратуры (ПК-10);

– способностью работать в международных проектах по тематике специализации (ПК-11);

– способностью участвовать в деятельности профессиональных сетевых сообществ по конкретным направлениям (ПК-12);

– социально ориентированная: способностью осознавать корпоративную политику в области повышения социальной ответственности бизнеса перед обществом, принимать участие в ее развитии (ПК-13);

– социально ориентированная деятельность: способность использования основ защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий и применения современных средств поражения, основных мер по ликвидации их последствий, способность к общей оценке условий безопасности жизнедеятельности (ПК-13);

– способность реализации решений, направленных на поддержку социально значимых проектов, на повышение электронной грамотности населения, обеспечения общедоступности информационных услуг (ПК-14).

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью освоения дисциплины «Модели и алгоритмы защиты информации» является формирование общекультурных и профессиональных компетенций, необходимых для реализации преимущественно следующих видов деятельности: научной и научно-исследовательской, а также педагогической:

ОК-4 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение.

ОК-9 Способность использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально-значимых проектов.

ПК-2 Способность разрабатывать концептуальные и теоретические модели решаемых научных проблем и задач.

Задачами изучения дисциплины выступает приобретение в рамках освоения теоретического и практического материала по дисциплине

Знаний:

- классических разделов математической науки;
- базовых идей и методов математики;
- системы основных математических структур и методов.
- критерий качества математических исследований, принципов экспериментальной и эмпирической проверки научных теорий.
- основополагающих фактов элементарной теории чисел, лежащих в основе построения всей математики; современные приложения теории чисел в области защиты информации.

Умений:

- реализовывать основные методы математических рассуждений на основе общих методов научного исследования и опыта решения учебных и научных проблем;
- пользоваться языком математики; корректно выражать и аргументировано обосновывать имеющиеся знания.
- пользоваться построением математических моделей для решения практических проблем; использовать рациональные способы получения, преобразования, систематизации и хранения информации, актуализировать ее в необходимых ситуациях интеллектуально-познавательной и профессиональной деятельности.
- анализировать существующие алгоритмы с точки зрения их эффективности и применимости для решения прикладных задач; разрабатывать новые алгоритмы для решения конкретных задач в области защиты информации; оценивать сложность разработанных алгоритмов и обосновывать их корректность.

Владений:

- культурой математического мышления; логической и алгоритмической культурой; основными положениями истории развития математики, эволюции математических идей и концепциями современной математической науки

- математикой как универсальным языком науки, средством моделирования явлений и процессов.

- навыками разработки основных теоретико-числовых алгоритмов на основе функционально логических языков программирования.

Содержание дисциплины охватывает круг вопросов, связанных с основными фактами элементарной теории чисел и их приложениями к защите информации.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ «МОДЕЛИ И АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Самостоятельная работа обучающихся является неотъемлемым элементом изучения дисциплины. В ходе самостоятельной работы происходит формирование знаний, умений и навыков в учебной, научно-исследовательской, профессиональной деятельности, формирование общекультурных и профессиональных компетенций будущего магистра.

Самостоятельная работа обучающихся предполагает изучение теоретического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение доступной учебной и научной литературы.

Самостоятельно изученные теоретические материалы повышают уровень подготовки обучающегося к усвоению лекционного материала и используются при выполнении лабораторных работ. В процессе самостоятельной работы обучающиеся:

- осваивают материал, предложенный им на лекциях с привлечением указанной преподавателем литературы;
- осваивают дополнительные теоретические вопросы связанные с алгебраическими структурами, используемыми в современных теориях кодирования и информации;
- осваивают новые принципы алгоритмического мышления в соответствии с парадигмой функционального программирования;
- готовятся к лабораторным занятиям в соответствии с описанием лабораторных работ и методическими указаниями к лабораторным работам;
- готовятся к защите выполненных работ с подготовкой отчёта о проделанной работе в соответствии с указаниями по оформлению отчёта;
- ведут подготовку к промежуточной аттестации по данному курсу, которая проходит в форме зачета (2 семестр) и экзамена (3 семестр).

Целями самостоятельной работы обучающегося являются:

- формирование навыков самостоятельной образовательной деятельности;
- выявления и устранения обучающимся пробелов в знаниях, необходимых для изучения данного курса;
- осознания роли и места изучаемой дисциплины в образовательной программе, по которой производится обучение.

Общие требования

Самостоятельная работа обучающегося должна быть обеспечена необходимыми учебными и методическими материалами:

- основной и дополнительной литературой;
- демонстрационными материалами, используемыми во время лекционных занятий;
- методическими указаниями по проведению лабораторных работ;
- перечнем вопросов, выносимых на промежуточную аттестацию.

Самостоятельная работа обучающегося способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Виды самостоятельной работы обучающихся

В рамках дисциплины применяются следующие виды самостоятельной работы:

1. Подготовка к лабораторным работам (для овладения новыми знаниями в рамках изучаемой дисциплины).
2. Оформление отчётов по лабораторным работам (для закрепления и систематизации полученных знаний, формирования навыков и умений).
3. Самостоятельное изучение тем раздела (для овладения новыми знаниями).
4. Подготовка к зачёту (для актуализации и систематизации учебного материала).

1. Подготовка к лабораторным работам

Лабораторные работы составляют важную часть теоретической и профессиональной практической подготовки обучающихся. Они направлены на формирование учебных и профессиональных практических умений. При подготовке к лабораторным занятиям обучающимся необходимо изучить основную литературу, ознакомиться с дополнительной литературой, с ресурсами информационно-телекоммуникационной сети «Интернет». При этом обучающийся должен учесть рекомендации преподавателя и требования учебной программы. В ходе подготовки к лабораторным занятиям необходимо освоить основные понятия; изучить алгоритмы; методы и технологии, необходимые для реализации этих алгоритмов; ответить на контрольные вопросы.

2. Оформление отчётов по лабораторным работам

В течении лабораторного занятия обучающемуся необходимо выполнить индивидуальные задания, выданные преподавателем, а затем оформить выполнение работы в виде отчёта в соответствии с нижеизложенными *указаниями по оформлению отчётов.*

1. Отчеты по лабораторным работам готовятся в электронном виде.
2. Отчет должен включать титульный лист и результаты выполнения лабораторных работ за весь семестр.
3. В отчете по каждой лабораторной работе указываются:
    - формулировка задания;
    - программный код;
    - результат выполнения программы в соответствии с индивидуальным вариантом;
    - оценка количества шагов алгоритма и его эффективность.
4. Отчеты по всем лабораторным работам сдаются преподавателю в конце семестра.

Защита лабораторных работ осуществляется демонстрацией выполненных работ, ответами на контрольные вопросы и отчётами по лабораторным работам. Защита лабораторных работ осуществляется обучающимся по мере выполнения лабораторных работ и относится к самостоятельной работе обучающегося под руководством преподавателя.

3. Самостоятельное изучение тем раздела

Организация самостоятельной работы по освоению содержания курса включает в себя такие виды работ как самостоятельное изучение текстов лекций, учебников из списка основной и дополнительной рекомендуемой литературы, использование ресурсов информационно-телекоммуникационной сети «Интернет» и пр. Имеет смысл ознакомиться с раскрытием содержания каждой лекции по нескольким рекомендованным источникам для сопоставления точек зрения различных авторов с различных методологических позиций, а для более углубленного изучения воспользоваться дополнительной литературой. Целесообразно также составление индивидуального терминологического словаря (глоссария) по теме вопросов, вынесенных на самостоятельное изучение, и словаря новых понятий, с которыми обучающийся впервые сталкивается в своей образовательной практике.

Для успешного освоения вопросов, вынесенных на самостоятельное изучение, необходимо законспектировать предложенные вопросы (см. перечень тем для самостоятельного изучения, предложенный в п. 4 рабочей программы дисциплины),

проанализировать различные подходы на изложение предложенной проблемы. Возможно использование литературы, подобранной самим обучающимся.

4. Подготовка к зачёту (2 семестр)

При подготовке к зачёту обучающийся в короткий срок прорабатывает содержание лекций по своему конспекту и, при необходимости, по рекомендованным учебникам. На каждый вопрос обучающийся должен написать план ответа, кратко перечислить и запомнить основные факты и положения. На этапе подготовки к зачёту обучающийся систематизирует и интегрирует информацию, относящуюся к разным разделам лекционного материала, лучше понимает взаимосвязь различных фактов и положений дисциплины, восполняет пробелы в своих знаниях.

Советы по планированию и организации времени,
необходимого для изучения дисциплины

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

- Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.
- Изучение конспекта лекции за день перед следующей лекцией – 10-15 минут.
- Изучение теоретического материала по учебнику и конспекту – 1 час в неделю (2 семестр); 2 часа в неделю (3 семестр).
- Подготовка к лабораторной работе – 1 час в неделю (3 семестр).

  Всего в неделю – 1 часа 30 минут (2 семестр); 3 часа 30 минут (3 семестр).

Описание последовательности действий обучающегося
(«сценарий изучения дисциплины»)

Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).
3. В течение недели выбрать время (1 час) для работы с литературой в библиотеке.
4. При подготовке к лабораторным занятиям следующего дня, необходимо сначала прочитать основные понятия и подходы по теме лабораторной работы. При

подготовке к выполнению лабораторной работы нужно сначала понять, что и как требуется сделать, какой теоретический материал нужно использовать, наметить план решения задачи.

Заключение

Самостоятельная работа обучающихся является одной из важнейших составляющих учебного процесса, в ходе которого происходит формирование знаний, умений и навыков в учебной, научно- исследовательской, профессиональной деятельности, формирование общекультурных и профессиональных компетенций будущего магистра. Учебно-методическое обеспечение создаёт среду актуализации самостоятельной творческой активности обучающихся, вызывает потребность к самопознанию, самообучению. Таким образом, создаются предпосылки «двойной подготовки» – личностного и профессионального становления. Для успешного осуществления самостоятельной работы необходимы:

1) Комплексный подход организации самостоятельной работы по всем формам аудиторной работы;
2) Сочетание всех уровней (типов) самостоятельной работы, предусмотренных рабочей программой;
3) Обеспечение контроля за качеством усвоения.

Рекомендации по самостоятельной работе

При самостоятельной работе рекомендуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и информационно-телекоммуникационной сети «Интернет», является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Имеет смысл ознакомиться с раскрытием содержания каждой лекции по нескольким рекомендованным источникам для сопоставления точек зрения различных авторов с различных методологических позиций, а для более углубленного изучения воспользоваться дополнительной литературой. Целесообразно также составление индивидуального терминологического словаря (глоссария) по теме вопросов, вынесенных на самостоятельное

изучение, и словаря новых понятий, с которыми обучающийся впервые сталкивается в своей образовательной практике.

Для успешного освоения вопросов, вынесенных на самостоятельное изучение, необходимо законспектировать предложенные вопросы (см. перечень тем для самостоятельного изучения, предложенный в п. 4 рабочей программы дисциплины), проанализировать различные подходы на изложение предложенной проблемы. Возможно использование литературы, подобранной самим обучающимся.

Рекомендации по выполнению лабораторных работ

Лабораторные работы составляют важную часть теоретической и профессиональной практической подготовки обучающихся. Они направлены на формирование учебных и профессиональных практических умений. На лабораторных занятиях задания выполняются по материалам согласно плану.

До начала лабораторных занятий обучающиеся должны пройти инструктаж по технике безопасности. Перед выполнением лабораторной работы обучающийся должен изучить теоретический материал по теме лабораторной работы по основной и дополнительной литературе, ознакомиться с ресурсами информационно-телекоммуникационной сети «Интернет». При этом обучающийся должен учесть рекомендации преподавателя и требования учебной программы. В ходе подготовки к лабораторным занятиям необходимо ознакомиться с методическими указаниями; с порядком ее выполнения; освоить основные понятия; изучить алгоритмы; методы и технологии, необходимые для реализации этих алгоритмов; ответить на контрольные вопросы.

Отчёт по лабораторной работе оформляется в соответствии с требованиями, указанными в методических указаниях к лабораторной работе.

Рекомендации по работе с литературой и использованию материалов учебно-методического комплекса

Рекомендуется использовать методические указания по курсу, текст лекций преподавателя. Однако теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги. Легче освоить курс придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, что даст это на практике?.

Рекомендации по подготовке к зачёту

Существуют общепринятые правила подготовки и сдачи студентами зачетов. Готовиться к зачету необходимо в течение всего учебного времени, т.е. с первого дня очередного семестра: вся работа студента на лекциях, лабораторных работах и т.п. это и есть этапы подготовки студента к зачету.

Подготовка к сессии должна быть нацелена не столько на приобретение новых знании, сколько на закрепление ранее изученного материала и повторение ею. Сумму полученных знаний студенту перед сессией надо разумно обобщить, привести в систему, закрепить и памяти, для чего ему надо использовать учебники, лекции, методические пособия и различного рода руководства. Повторение необходимо производить но разделам, темам.

Дополнительно к изучению конспектов лекции необходимо пользоваться учебником. Кроме «заучивания» материала зачёта или экзамена, очень важно добиться состояния понимания изучаемых тем дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, что даст это на практике?.

При подготовке к зачету нужно изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала и самостоятельно решить по нескольку типовых задач из каждой темы. При решении задач всегда необходимо уметь качественно интерпретировать итог решения.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ «МОДЕЛИ И АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛЕКЦИОННЫМ ЗАНЯТИЯМ

Лекция представляет собой систематическое устное изложение учебного материала. С учетом целей и места в учебном процессе различают лекции вводные, установочные, текущие, обзорные и заключительные. В зависимости от способа проведения выделяют лекции:

— *Информационные;*
— *Проблемные;*
— *Визуальные;*
— *бинарные (лекция-диалог);*
— *лекции-провокации;*
— *лекции-конференции;*
— *лекции-консультации;*
— *лекции-беседы;*
— *лекция с эвристическими элементами;*
— *лекция с элементами обратной связи;*
— *лекция с решением производственных и конструктивных задач;*
— *лекция с элементами самостоятельной работы студентов;*
— *лекция с решением конкретных ситуаций;*
— *лекция с коллективным исследованием;*
— *лекции спецкурсов*.

При чтении лекций по дисциплине «Модели и алгоритмы защиты информации», используются следующие способы представления материала:

- ✓ *информационные* – проводятся с использованием объяснительно иллюстративного метода изложения; это традиционный для высшей школы тип лекций;
- ✓ *визуальные* – предполагают визуальную подачу материала техническими средствами обучения, аудио- и видеотехники, мультимедийных технологий, с кратким комментированием демонстрируемых материалов;
- ✓ *лекции-беседы.* В названном виде занятий планируется диалог с аудиторией, это наиболее простой способ индивидуального общения, построенный на непосредственном контакте преподавателя и студента, который позволяет привлекать к двухстороннему обмену мнениями по наиболее важным вопросам темы занятия, менять темп изложения с учетом особенности аудитории. В начале лекции и по ходу ее преподаватель задает слушателям вопросы не для контроля усвоения знаний, а для выяснения уровня осведомленности по рассматриваемой проблеме. Вопросы могут быть элементарными: для того, чтобы сосредоточить внимание, как на отдельных нюансах темы, так и на проблемах. Продумывая ответ, студенты получают возможность самостоятельно прийти к выводам и обобщениям, которые хочет сообщить преподаватель в качестве новых знаний.

Необходимо следить, чтобы вопросы не оставались без ответа, иначе лекция будет носить риторический характер.

- ✓ *лекция с элементами обратной связи.* В данном случае подразумевается изложение учебного материала и использование знаний по смежным предметам (межпредметные связи) или по изученному ранее учебному материалу. Обратная связь устанавливается посредством ответов студентов на вопросы преподавателя по ходу лекции. Чтобы определить осведомленность студентов по излагаемой проблеме, в начале какого-либо раздела лекции задаются необходимые вопросы.

Если студенты правильно отвечают на вводный вопрос, преподаватель может ограничиться кратким тезисом или выводом и перейти к следующему вопросу.

Если же ответы не удовлетворяют уровню желаемых знаний, преподаватель сам излагает подробный ответ, и в конце объяснения снова задает вопрос, определяя степень усвоения учебного материала.

Если ответы вновь демонстрируют низкий уровень знаний студентов – следует изменить методику подачи учебного материала.

Написание конспекта лекций:

Конспект представляет собой относительно подробное, последовательное изложение содержания прочитанного. На первых порах целесообразно в записях ближе держаться тексту, прибегая зачастую к прямому цитированию автора. В дальнейшем, по мере выработки навыков конспектирования, записи будут носить более свободный и сжатый характер.

Конспект подразделяется на части в соответствии с заранее продуманным планом. В первую очередь необходимо составить план произведения письменно или мысленно, поскольку в соответствии с этим планом строится дальнейшая работа.

Лекции являются эффективным видом занятий для формирования у студентов способности быстро воспринимать новые факты, идеи, обобщать их, а также самостоятельно мыслить.

Лектор излагает теоретический и практический материал, относящийся к основному курсу. Из большого числа монографий, учебников, сборников лектор выбирает самое главное, помогает усвоить логику рассуждений. Интонацией голоса и манерой изложения лектором подчеркивает наиболее существенное, выделяет главное и второстепенное.

Студенту следует научиться понимать и основную идею лекции, а также, следуя за лектором, участвовать в усвоении новых мыслей. Но для этого надо быть подготовленным к восприятию очередной темы. Время, отведенное на лекцию, можно считать использованным полноценно, если студенты понимают роль лектора, задачи лекции, если работают вместе с лектором, а не бездумно ведут конспект.

Подготовленным можно считать такого студента, который, присутствуя на лекции, усвоил ее содержание, а перед лекцией припомнил материал раздела, излагаемого на ней или просмотрел свой конспект, или учебник.

Перед лекцией необходимо прочитывать конспект предыдущей лекции, а после окончания крупного раздела курса рекомендуется проработать его по конспектам и учебникам.

Для наиболее важных дисциплин, вызывающих наибольшие затруднения, рекомендуется перед каждой лекцией просматривать содержание предстоящей лекции по

учебнику с тем, чтобы лучше воспринять материал лекции. В этом случае предмет усваивается настолько, что перед экзаменом остается сделать немногое для закрепления знаний.

1. Рекомендации по конспектированию лекций

Лекции являются эффективным видом занятий для формирования у студентов способности быстро воспринимать новые факты, идеи, обобщать их, а также самостоятельно мыслить.

Лектор излагает теоретический и практический материал, относящийся к основному курсу. Из большого числа монографий, учебников, сборников лектор выбирает самое главное, помогает усвоить логику рассуждений. Интонацией голоса и манерой изложения лектором подчеркивает наиболее существенное, выделяет главное и второстепенное. Наиболее важные положения лекции записываются под диктовку лектора.

Студенту следует научиться понимать и основную идею лекции, а также, следуя за лектором, участвовать в усвоении новых мыслей. Но для этого надо быть подготовленным к восприятию очередной темы. Время, отведенное на лекцию, можно считать использованным полноценно, если студенты понимают задачи лекции, если работают вместе с лектором, а не бездумно ведут конспект.

Подготовленным можно считать такого студента, который, присутствуя на лекции, усвоил ее содержание, а перед лекцией просмотрел конспект предыдущей лекции или учебник. После окончания крупного раздела курса рекомендуется проработать его по конспектам и учебникам.

Для наиболее важных дисциплин, вызывающих наибольшие затруднения, рекомендуется перед каждой лекцией просматривать содержание предстоящей лекции по учебнику с тем, чтобы лучше воспринять материал лекции. В этом случае предмет усваивается настолько, что перед экзаменом остается сделать немногое для закрепления знаний.

РАЗДЕЛ 1. АЛГОРИТМЫ ТЕОРИИ ДЕЛИМОСТИ И СРАВНЕНИЙ

Лекция 1. Элементарная теория делимости

Основные темы

Операция деления, деление с остатком.

Наибольший общий делитель, его свойства.

Алгоритм Евклида. Теорема Ламе.

Двоичный алгоритм Евклида.

Простые числа.

Основная теорема арифметики.

РАЗДЕЛ 1. АЛГОРИТМЫ ТЕОРИИ ДЕЛИМОСТИ И СРАВНЕНИЙ

Лекция 2. Сравнения

Основные темы

Вычеты по модулю целых чисел.

Теорема о числе решений сравнения первой степени.

Лемма Безу.

Расширенный алгоритм Евклида.
Китайская теорема об остатках.
Алгоритм Гарнера.
Функция Эйлера.
Теоремы Эйлера и Ферма.
Первообразные корни.
Теорема о существовании первообразного корня по модулю простого числа.

РАЗДЕЛ 1. АЛГОРИТМЫ ТЕОРИИ ДЕЛИМОСТИ И СРАВНЕНИЙ

Лекция 3. Многочлены

Основные темы

Определение элементарных операций.
Алгоритмы умножения многочленов.
Операция деления с остатком для многочленов.
Алгоритм Евклида для многочленов.
Лемма Безу для многочленов.
Основная теорема арифметики для многочленов.
Теорема о числе корней многочленов.
Теоремы о подъеме решений.

РАЗДЕЛ 1. АЛГОРИТМЫ ТЕОРИИ ДЕЛИМОСТИ И СРАВНЕНИЙ

Лекция 4. Сравнения старших степеней

Основные темы

Определение квадратичного вычета.
Символ Лежандра.
Теорема о числе решений.
Свойства символа Лежандра.
Определение символа Якоби, его свойства.
Алгоритм вычисления символа Якоби.

РАЗДЕЛ 1. АЛГОРИТМЫ ТЕОРИИ ДЕЛИМОСТИ И СРАВНЕНИЙ

Лекция 5. Сравнения старших степеней (продолжение)

Основные темы

Вычисление квадратного корня: частные случаи.
Алгоритм Тонелли-Шенкса.
Общее квадратное уравнение.
Вероятностный алгоритм вычисления корней многочлена.

РАЗДЕЛ 2. ТЕОРЕТИКО-ЧИСЛОВЫЕ АЛГОРИТМЫ

Лекция 6. Простые числа

Основные темы

Построение таблицы простых чисел.

Вероятностные алгоритмы проверки на простоту.
Тест Соловея–Штрассена.
Тест Миллера–Рабина.
Теорема Поклингтона и ее дополнения.
Алгоритмы построения простых чисел.
Реккурентные последовательности Люка.
Теорема Моррисона.
Рекурсивный алгоритм построения простого числа с известным разложением $p-1$.
Алгоритм построения сильно простого числа.

РАЗДЕЛ 2. ТЕОРЕТИКО-ЧИСЛОВЫЕ АЛГОРИТМЫ

Лекция 7. Непрерывные дроби

Основные темы

Определение непрерывной дроби.
Понятие подходящей дроби.
Теорема о наилучшем приближении.
Квадратичные иррациональности и их свойства.
Подходящие дроби и наилучшие приближения.

РАЗДЕЛ 2. ТЕОРЕТИКО-ЧИСЛОВЫЕ АЛГОРИТМЫ

Лекция 8. Факторизация целых чисел

Основные темы

Метод пробного деления.
Метод Ферма.
Метод Лемана.
Метод Полларда.
Метод Брента.
$p-1$ метод Полларда.
$p+1$ метод Вильямса.
Оптимизация методов Полларда и Вильямса.

РАЗДЕЛ 2. ТЕОРЕТИКО-ЧИСЛОВЫЕ АЛГОРИТМЫ

Лекция 9. Факторизация целых чисел (продолжение)

Основные темы

Метод Женга. Метод Макки.
Основная лемма факторизации.
Решето (метод) Крайчика.
Метод непрерывных дробей.
Метод Моррисона–Брилхарда.
Линейное решето Шреппеля. Квадратичное решето.

РАЗДЕЛ 3. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Лекция 10. Традиционные шифры с симметричным ключом

Основные темы

Основные понятия криптографии.
Криптоанализ и типы атак.
Шифры подстановки.
Криптоанализ шифров подстановок.
Шифры перестановок.
Криптоанализ шифров перестановки.
Шифры потока и блочные шифры.

РАЗДЕЛ 3. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Лекция 11. Современные блочные шифры и шифры потока.

Основные темы

Полноразмерные ключевые шифры.
Шифры ключа частичного размера.
Шифры без ключа.
Шифры Файстеля.
Шифры не-Файстеля.
Атаки на блочные шифры.
Синхронные шифры потока.

РАЗДЕЛ 3. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Лекция 12. Шифр DES (Data Encryption Standard)

Основные темы

Общие положения шифра DES.
Структура и алгоритмы DES.
Анализ DES.
Многократное применение DES.
Безопасность DES.

РАЗДЕЛ 3. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Лекция 13. Шифр AES (Advanced Encryption Standard)

Основные темы

Общие положения шифра AES.
Преобразования в шифре AES.

РАЗДЕЛ 3. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Лекция 14. Шифр AES (продолжение)

Основные темы

Расширение ключей AES (AES-128, AES-192 и AES-256).
Алгоритмы шифра и обратного шифра AES.

Анализ AES.

РАЗДЕЛ 3. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Лекция 15. Применение современных шифров с симметричным ключом

Основные темы

Применение современных блочных шифров.

Использование шифров потока.

Проблемы управлением и генерацией ключей.

РАЗДЕЛ 3. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Лекция 16. Алгоритм асимметрично-ключевой криптографии

Основные темы

Основные идеи и положения асимметрично-ключевой криптографии.

Криптографическая система RSA.

Атаки на RSA.

Написание конспекта лекций необходимо проводить кратко, схематично; последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Незнакомые термины, понятия после лекции проверять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или на лабораторном занятии.

Желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

Подготовка к лабораторной работе 1. Элементарная теория делимости.

Реализация алгоритма 1.1 (Алгоритм Евклида).

Реализация алгоритма 1.2 (Бинарный алгоритм вычисления НОД).

Цели и задачи лабораторной работы: Реализовать, рассмотренные на лекционных занятиях, алгоритмы с помощью функционального языка программирования Sheme. Оценить количество шагов и эффективность алгоритма.

Теоретические основы. Лабораторная работа 1 относится к разделу «Алгоритмы теории делимости и сравнений». При подготовке к занятию необходимо проанализировать информацию по теме «Элементарная теория делимости»: Операция деления, деление с остатком. Наибольший общий делитель, его свойства. Алгоритм Евклида. Теорема Ламе. Двоичный алгоритм Евклида. Простые числа. Основная теорема арифметики.

Ход подготовки к лабораторной работе. Требуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и информационно-телекоммуникационной сети «Интернет», является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Подготовка к лабораторной работе 2. Сравнения

Реализация алгоритма 2.1 (Расширенный алгоритм Евклида).

Реализация алгоритма 2.2 (Китайская теорема об остатках).

Реализация алгоритма 2.3 (Алгоритм Гарнера).

Реализация алгоритма 2.4 (Вычисление первообразного корня).

Цели и задачи лабораторной работы: Реализовать, рассмотренные на лекционных занятиях, алгоритмы с помощью функционального языка программирования Sheme. Оценить количество шагов и эффективность алгоритма.

Теоретические основы. Лабораторная работа 2 относится к разделу «Алгоритмы теории делимости и сравнений». При подготовке к занятию необходимо проанализировать информацию по теме «Сравнения»: Вычеты по модулю целых чисел. Теорема о числе

решений сравнения первой степени. Лемма Безу. Расширенный алгоритм Евклида. Китайская теорема об остатках. Алгоритм Гарнера. Функция Эйлера. Теоремы Эйлера и Ферма. Первообразные корни. Теорема о существовании первообразного корня по модулю простого числа.

Ход подготовки к лабораторной работе. Требуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и информационно-телекоммуникационной сети «Интернет», является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Подготовка к лабораторной работе 3. Многочлены

Реализация алгоритма 3.1 (Деление многочленов с остатком).

Реализация алгоритма 3.2 (Алгоритм Эвклида для многочленов).

Реализация алгоритма 3.3 (Алгоритм поднятия решения).

Цели и задачи лабораторной работы: Реализовать, рассмотренные на лекционных занятиях, алгоритмы с помощью функционального языка программирования Sheme. Оценить количество шагов и эффективность алгоритма.

Теоретические основы. Лабораторная работа 3 относится к разделу «Алгоритмы теории делимости и сравнений». При подготовке к занятию необходимо проанализировать информацию по теме «Многочлены»: Определение элементарных операций. Алгоритмы умножения многочленов. Операция деления с остатком для многочленов. Алгоритм Евклида для многочленов. Лемма Безу для многочленов. Основная теорема арифметики для многочленов. Теорема о числе корней многочленов. Теоремы о подъеме решений.

Ход подготовки к лабораторной работе. Требуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и информационно-телекоммуникационной сети «Интернет», является наиболее эффективным

методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Подготовка к лабораторной работе 4. Сравнения старших степеней

Реализация алгоритма 4.1 (Вычисление символа Якоби).

Реализация алгоритма 4.2 (Алгоритм Тонелли–Шенкса).

Реализация алгоритма 4.3 (Вычисление случайного корня многочлена).

Реализация алгоритма 4.4 (Вычисление всех корней многочлена).

Цели и задачи лабораторной работы: Реализовать, рассмотренные на лекционных занятиях, алгоритмы с помощью функционального языка программирования Sheme. Оценить количество шагов и эффективность алгоритма.

Теоретические основы. Лабораторная работа 4 относится к разделу «Алгоритмы теории делимости и сравнений». При подготовке к занятию необходимо проанализировать информацию по теме «Сравнения старших степеней»: Определение квадратичного вычета. Символ Лежандра. Теорема о числе решений. Свойства символа Лежандра. Определение символа Якоби, его свойства. Алгоритм вычисления символа Якоби. Вычисление квадратного корня: частные случаи. Алгоритм Тонелли-Шенкса. Общее квадратное уравнение. Вероятностный алгоритм вычисления корней многочлена.

Ход подготовки к лабораторной работе. Требуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и информационно-телекоммуникационной сети «Интернет», является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Подготовка к лабораторной работе 5. Простые числа

Реализация алгоритма 5.1 (Алгоритм построения таблицы простых чисел).

Реализация алгоритма 5.2 (Тест Соловея–Штрассена).

Реализация алгоритма 5.3 (Тест Миллера–Рабина).

Реализация алгоритма 5.4 (Алгоритм Люка для доказательства простоты).

Цели и задачи лабораторной работы: Реализовать, рассмотренные на лекционных занятиях, алгоритмы с помощью функционального языка программирования Sheme. Оценить количество шагов и эффективность алгоритма.

Теоретические основы. Лабораторная работа 5 относится к разделу «Теоретико-числовые алгоритмы». При подготовке к занятию необходимо проанализировать информацию по теме «Простые числа»: Построение таблицы простых чисел. Вероятностные алгоритмы проверки на простоту. Тест Соловея–Штрассена. Тест Миллера–Рабина. Теорема Поклингтона и ее дополнения. Алгоритмы построения простых чисел. Реккурентные последовательности Люка. Теорема Моррисона. Рекурсивный алгоритм построения простого числа с известным разложением $p-1$. Алгоритм построения сильно простого числа.

Ход подготовки к лабораторной работе. Требуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и информационно-телекоммуникационной сети «Интернет», является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Подготовка к лабораторной работе 6. Простые числа (продолжение)

Реализация алгоритма 5.5 (Вычисление последовательностей Люка).

Реализация алгоритма 5.6 (Алгоритм построения простого числа).

Реализация алгоритма 5.7 (Алгоритм построения сильно простого числа).

Цели и задачи лабораторной работы: Реализовать, рассмотренные на лекционных занятиях, алгоритмы с помощью функционального языка программирования Sheme. Оценить количество шагов и эффективность алгоритма.

Теоретические основы. Лабораторная работа 6 относится к разделу «Теоретико-числовые алгоритмы». При подготовке к занятию необходимо проанализировать информацию по теме «Простые числа»: Построение таблицы простых чисел. Вероятностные алгоритмы проверки на простоту. Тест Соловея–Штрассена. Тест Миллера–Рабина. Теорема Поклингтона и ее дополнения. Алгоритмы построения простых чисел. Реккурентные последовательности Люка. Теорема Моррисона. Рекурсивный алгоритм построения простого числа с известным разложением $p-1$. Алгоритм построения сильно простого числа.

Ход подготовки к лабораторной работе. Требуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и информационно-телекоммуникационной сети «Интернет», является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Подготовка к лабораторной работе 7. Факторизация целых чисел

Реализация алгоритма 7.1 (Алгоритм факторизации Ферма).

Реализация алгоритма 7.2 (Вычисление целозначного квадратного корня).

Реализация алгоритма 7.3 (Алгоритм Лемана).

Реализация алгоритма 7.4 (Метод Полларда-Флойда).

Реализация алгоритма 7.5 (Алгоритм Брента).

Реализация алгоритма 7.6 (p–1 алгоритм факторизации Вильямса).

Реализация алгоритма 7.7 (p+1 алгоритм факторизации Вильямса).

Цели и задачи лабораторной работы: Реализовать, рассмотренные на лекционных занятиях, алгоритмы с помощью функционального языка программирования Sheme. Оценить количество шагов и эффективность алгоритма.

Теоретические основы. Лабораторная работа 7 относится к разделу «Теоретико-числовые алгоритмы». При подготовке к занятию необходимо проанализировать информацию по теме «Факторизация целых чисел»: Метод пробного деления. Метод Ферма. Метод Лемана. Метод Полларда. Метод Брента. $p-1$ метод Полларда. $p+1$ метод Вильямса. Оптимизация методов Полларда и Вильямса. Метод Женга. Метод Макки. Основная лемма факторизации. Решето (метод) Крайчика. Метод непрерывных дробей. Метод Моррисона–Брилхарда. Линейное решето Шреппеля. Квадратичное решето.

Ход подготовки к лабораторной работе. Требуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и

информационно-телекоммуникационной сети «Интернет», является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Подготовка к лабораторной работе 8.

Традиционные шифры с симметричным ключом

Реализация алгоритма 8.1 (Метод замены).

Реализация алгоритма 8.2 (Метод многоалфавитной замены).

Реализация алгоритма 8.3 (Метод гаммирования).

Цели и задачи лабораторной работы: Реализовать, рассмотренные на лекционных занятиях, алгоритмы с помощью функционального языка программирования Sheme. Оценить количество шагов и эффективность алгоритма.

Теоретические основы. Лабораторная работа 8 относится к разделу «Криптографические алгоритмы». При подготовке к занятию необходимо проанализировать информацию по теме «Традиционные шифры с симметричным ключом»: Основные понятия криптографии. Криптоанализ и типы атак. Шифры подстановки. Криптоанализ шифров подстановок. Шифры перестановок. Криптоанализ шифров перестановки. Шифры потока и блочные шифры

Ход подготовки к лабораторной работе. Требуется изучить конспекты лекций и усвоить полученную информацию. Необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Возможно использование литературы, подобранной самим обучающимся. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и информационно-телекоммуникационной сети «Интернет», является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Список программного обеспечения необходимого для выполнения лабораторной работы

1. Операционная система GNU/Linux с ядром не ниже 2.6.32 или операционная система Windows NT 5.1 (Windows XP) и выше.
2. Среда разработки DrRacket (DrScheme) v4.2.1 и выше.

3. Текстовый процессор LibreOffice Writer v3.5.7 и выше.

Для выполнения лабораторной работы необходим компьютерный класс с соответствующим (необходимым для выполнения лабораторной работы) программным обеспечением

1. Операционная система GNU/Linux с ядром не ниже 2.6.32 или операционная система Windows NT 5.1 (Windows XP) и выше.
2. Среда разработки DrRacket (DrScheme) v4.2.1 и выше.
3. Текстовый процессор LibreOffice Writer v3.5.7 и выше.

СОДЕРЖАНИЕ

ВОПРОСЫ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Примерный перечень вопросов к зачету

1. Операция деления, деление с остатком.
2. Наибольший общий делитель, его свойства.
3. Алгоритм Евклида.
4. Теорема Ламе.
5. Двоичный алгоритм Евклида.
6. Простые числа.
7. Основная теорема арифметики.
8. Вычеты по модулю целых чисел.
9. Теорема о числе решений сравнения первой степени.
10. Лемма Безу.
11. Расширенный алгоритм Евклида.
12. Китайская теорема об остатках.
13. Алгоритм Гарнера.
14. Функция Эйлера.
15. Теоремы Эйлера и Ферма.
16. Первообразные корни.
17. Теорема о существовании первообразного корня по модулю простого числа.
18. Определение элементарных операций над многочленами.
19. Алгоритмы умножения многочленов.
20. Операция деления с остатком для многочленов.
21. Алгоритм Евклида для многочленов.
22. Лемма Безу для многочленов.
23. Основная теорема арифметики для многочленов.
24. Теорема о числе корней многочленов.
25. Теоремы о подъеме решений.
26. Определение квадратичного вычета.
27. Символ Лежандра.
28. Теорема о числе решений.
29. Свойства символа Лежандра.
30. Определение символа Якоби, его свойства.
31. Алгоритм вычисления символа Якоби.
32. Вычисление квадратного корня: частные случаи.
33. Алгоритм Тонелли-Шенкса.
34. Общее квадратное уравнение.
35. Вероятностный алгоритм вычисления корней многочлена.
36. Построение таблицы простых чисел.
37. Вероятностные алгоритмы проверки на простоту.
38. Тест Соловея–Штрассена.
39. Тест Миллера–Рабина.
40. Теорема Поклингтона и ее дополнения.
41. Алгоритмы построения простых чисел.

42. Реккурентные последовательности Люка.
43. Теорема Моррисона.
44. Рекурсивный алгоритм построения простого числа с известным разложением $p-1$.
45. Алгоритм построения сильно простого числа.
46. Определение непрерывной дроби.
47. Понятие подходящей дроби.
48. Теорема о наилучшем приближении.
49. Квадратичные иррациональности и их свойства.
50. Подходящие дроби и наилучшие приближения.
51. Метод пробного деления (факторизации).
52. Метод факторизации Ферма.
53. Метод факторизации Лемана.
54. Метод факторизации Полларда.
55. Метод факторизации Брента.
56. $p-1$ метод факторизации Полларда.
57. $p+1$ метод факторизации Вильямса.
58. Оптимизация методов факторизации Полларда и Вильямса.
59. Метод факторизации Женга.
60. Метод факторизации Макки.
61. Основная лемма факторизации.
62. Решето (метод факторизации) Крайчика.
63. Метод непрерывных дробей (факторизация).
64. Метод факторизации Моррисона–Брилхарда.
65. Линейное решето Шреппеля (факторизация).
66. Квадратичное решето (факторизация).

Примерный перечень вопросов к экзамену

1. Основные понятия криптографии.
2. Криптоанализ и типы атак.
3. Шифры подстановки. Криптоанализ шифров подстановок.
4. Шифры перестановок. Криптоанализ шифров перестановки.
5. Шифры потока и блочные шифры.
6. Полноразмерные ключевые шифры.
7. Шифры ключа частичного размера.
8. Шифры без ключа. Шифры Файстеля. Шифры не-Файстеля.
9. Атаки на блочные шифры.
10. Синхронные шифры потока.
11. Общие положения шифра DES.
12. Структура и алгоритмы DES.
13. Анализ шифра DES.
14. Многократное применение шифра DES.
15. Безопасность шифра DES.
16. Общие положения шифра AES.
17. Преобразования в шифре AES.

18. Расширение шифра AES (AES-128, AES-192 и AES-256).
19. Алгоритмы шифра и обратного шифра AES.
20. Анализ шифра AES.
21. Применение современных блочных шифров.
22. Использование шифров потока.
23. Проблемы управлением и генерацией ключей.
24. Основные идеи и положения асимметрично-ключевой криптографии.
25. Криптографическая система RSA.
26. Атаки на RSA.

СОДЕРЖАНИЕ

ЗАКЛЮЧЕНИЕ

Выпускник по направлению подготовки 010400 Прикладная математика и информатика Самарского государственного технического университета отвечает следующим требованиям:

– имеет целостное представление о процессах и явлениях, происходящих в неживой и живой природе, понимает возможности современных научных методов познания природы и владеет ими на уровне, необходимом для решения задач, имеющих естественнонаучное содержание и возникающих при выполнении профессиональных функций;

– способен продолжить обучение в аспирантуре, вести профессиональную деятельность в иноязычной среде;

– владеет культурой мышления, знает его общие законы, способен в письменной и устной речи правильно (логически) оформить его результаты;

– умеет на научной основе организовать свой труд, владеет компьютерными методами сбора, хранения и обработки (редактирования) информации, применяемые в сфере его профессиональной деятельности;

– способен в условиях развития науки и изменяющейся социальной практики к переоценке накопленного опыта, анализу своих возможностей, умеет приобретать новые знания, обучаться в аспирантуре, использовать другие формы обучения, включая самостоятельные и информационно образовательные технологии;

– понимает сущность и социальную значимость своей будущей профессии, основные проблемы дисциплин, определяющих конкретную область его деятельности, видит их взаимосвязь в целостной системе знаний;

– способен к проектной деятельности в профессиональной сфере на основе системного подхода, умеет строить и использовать модели для описания и прогнозирования различных явлений, осуществлять их качественный и количественный анализ;

– способен поставить цель и сформулировать задачи, связанные с реализацией профессиональных функций, умеет использовать для их решения методы изученных им наук;

– готов к кооперации с коллегами и работе в коллективе, знаком с методами управления, умеет организовать работу исполнителей, находить и принимать управленческие решения в условиях различных мнений, знает основы педагогической деятельности;

– методически и психологически готов к изменению вида и характера своей профессиональной деятельности, работе над междисциплинарными проектами;

– знает основные тенденции развития современными естествознания, принципы математического моделирования и его применения в исследовании физических, химических, биологических, экологических процессов;

– способен к совершенствованию своей профессиональной деятельности в области математики, программирования.

СОДЕРЖАНИЕ

ЛИТЕРАТУРА

Основная литература

№ п/п	Учебник, учебное пособие (приводится библиографическое описание учебника, учебного пособия)	Ресурс НТБ СамГТУ	Кол-во экз.
1.	Виноградов И.М. Основы теории чисел: 12-е изд., стер. Спб.: Лань, 2009. 176 с.	ЭБС изд-ва Лань	Электр. Ресурс / 2 экз.
2.	Василенко О.Н. Теоретико-числовые алгоритмы в криптографии: 2-е доп. М.: МЦНМО, 2006. 336 с.	ЭБС изд-ва Лань	Электр. Ресурс
3.	Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. М.: СОЛОН-Пресс, 2009. 256 с.	ЭБС изд-ва Лань	Электр. Ресурс
4.	Глухов М.М., Круглов И.А., Пичкур А.Б., Черёмушкин А.В. Введение в теоретико-числовые методы криптографии. Спб. Лань, 2011. 400 с.	ЭБС изд-ва Лань	Электр. Ресурс

Дополнительная литература

№ п/п	Учебник, учебное пособие, монография, справочная литература (приводится библиографическое описание)	Ресурс НТБ СамГТУ	Кол-во экз.
1.	Бухштаб А. А. Теория чисел: учеб. пособие; 3-е изд., стер. СПб.: Лань, 2008. 384 с.	ЭБС изд-ва Лань	Электр. Ресурс / 1 экз.
2.	Фергюсон Н., Шнайер Б. Практическая криптография: Пер.с англ. Киев; М.; СПб.: Диалектика, 2005. 421 с.	004.056 Ф-431	3 экз.
3.	Громов Ю.Ю., Драчев В.О., Иванова О.Г., Шахов Н.Г. Информационная безопасность и защита информации: учеб. пособие. Старый Оскол: ТНТ, 2010. 383 с.	004.056(075.8) И-741	3 экз.
4.	Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 815 с	004.056 Ш-76	1 экз.
5.	Ингам А. Э. Распределение простых чисел: пер.с англ.; 4-е изд. М.: Либроком, 2009. 160 с.	511.3 И-59	1 экз.
6.	Земор Ж. Курс криптографии: пер.с фр. М.; Ижевск: Регуляр. и хаот. динамика : Ин-т компьютер. исслед., 2006. - 255 с.	004.056 З-548	1 экз.
7.	Хинчин А. Я. Избранные труды по теории чисел/ Под ред. Ю.В. Нестеренко. - М. : МЦНМО, 2006. - 260 с	511.2 Х-479	1 экз.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», содержащих дополнительную информацию:

1. Математика криптографии и теория шифрования: учебный курс на сайте Национального открытого университета ИНТУИТ (http://www.intuit.ru/studies/courses/552/408/info).
2. Основы криптографии: учебный курс на сайте Национального открытого университета ИНТУИТ (http://www.intuit.ru/studies/courses/691/547/info).
3. Основы теории информации и криптографии: учебный курс на сайте Национального открытого университета ИНТУИТ (http://www.intuit.ru/studies/courses/2256/140/info).
4. The Racket Language: официальный сайт Racket (http://racket-lang.org/).

СОДЕРЖАНИЕ

Саушкин Михаил Николаевич

Методические указания по дисциплине «Модели и алгоритмы защиты информации»

Электронные методические указания

Компьютерная верстка Е. В. Башкинова

Подписано для размещения в электронной библиотеке СамГТУ 25.12.2014

Формат 60x84 ⅛ .

Усл. п. л. .3,72_. Уч. -изд. л. 4,19.

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Самарский государственный технический университет»

443100. Самара, ул. Молодогвардейская, 244.

Главный корпус.

E-mail radch@samgtu.ru