МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

ПРОГРАММА

вступительного экзамена по специальной дисциплине,
соответствующей научной специальности аспирантуры

2.3.6. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Введение

В основе настоящей программы лежит материал следующих учебных дисциплин: дискретная математика, математическая логика, теория вероятностей, математическая статистика, алгоритмы и анализ сложности, базы данных и СУБД, моделирование информационных систем, основы информационной безопасности, теоретические основы компьютерной безопасности, организационно-правовое обеспечение защиты информации, информационное право, российские и международные стандарты безопасности информации, криптографические методы защиты информации, криптографические протоколы, теоретико-числовые методы в криптографии, защита операционных систем, защита информационных систем от вредоносных программ, проектирование и разработка приложений в защищенном исполнении, технические средства и методы защиты информации, защита баз данных, программно-аппаратные средства защиты информации, анализ уязвимостей программного обеспечения, защита компьютерных сетей, модели безопасности компьютерных систем.

Экзамен проводится по билетам, включающим два теоретических вопроса из разных разделов предложенной программы и третий вопрос – развернутое сообщение по теме планируемого или проводимого в настоящее время научного исследования. В основу ответа на третий вопрос могут быть положены публикации поступающего в аспирантуру; выпускная квалификационная работа, выполненная на предыдущем уровне обучения; иные исследовательские работы или подготовленный реферат.

Каждый вопрос оценивается по пятибалльной системе.

1. Математика

1. Булевы функции: основные тождества, СДНФ и СКНФ, полиномы Жегалкина, замкнутые классы T0, T1, S, L, M. Полная система булевых функций, базис, критерий полноты (формулировка).
2. Выводимость формулы из гипотез в исчислении высказываний и исчислении предикатов. Метод резолюций для проверки выводимости формулы из гипотез.
3. Функции, вычислимые и невычислимые по Тьюрингу. Тезис Черча-Тьюринга. Алгоритмически неразрешимые проблемы, примеры.
4. Экстремальные задачи теории графов: минимальное остовное дерево, кратчайший путь между вершинами, задача коммивояжера. Точные и приближенные алгоритмы для их решения: алгоритм Дейкстры, «жадные» алгоритмы.

5. Комбинаторные операции: сочетания и размещения (с возвращением и без возвращения элементов). Комбинаторные принципы: сложение, умножение, дополнение, включение-исключение. Бином Ньютона. Полиномиальная формула.

6. Алфавитное кодирование: необходимое и достаточные условия однозначности декодирования. Теорема и алгоритм Маркова. Коды Хаффмана и Хэмминга.

7. Конечные автоматы: задачи анализа и синтеза автоматов, автоматные функции и операции над ними (суперпозиция, введение обратной связи).

8. Аксиоматическое определение вероятности. Следствия из аксиом теории вероятностей.

9. Нормальное распределение. Его характеристики и свойства. Стандартное нормальное распределение. Сходимость по распределению. Асимптотическая нормальность. Центральная предельная теорема.

10. Точечное и доверительное оценивание параметрических функций. Методы получения точечных оценок для неизвестных параметров распределений: метод моментов, максимального правдоподобия, метод квантилей.

2. Программирование

1. Понятие дерева. Способы изображения деревьев. Способы представления деревьев. Обход дерева. Основные характеристики сбалансированных деревьев: идеально-сбалансированное дерево, АВЛ-дерево, красно-черное дерево, дерево случайного поиска, B-дерево.

2. Понятие графа. Способы изображения графов. Способы представления графов. Обход графа. Алгоритм нахождения кратчайшего пути в графе. Алгоритм нахождения множества достижимых вершин в графе.

3. Жизненный цикл программного обеспечения. Программы с большой и с малой жизнью. Этапы разработки программ по ГОСТ ЕСПД, по Майерсу. Технология макетирования. Модель водопада. Экстремальное программирование.

4. Автоматные грамматики. Конечные автоматы. Теорема Клини. Понятие регулярного выражения. Эквивалентность регулярных выражений и автоматных грамматик.

5. Контекстно-свободные грамматики. Учет самовложения в алгоритмах распознавания. Метод рекурсивного спуска при анализе грамматики. LL-грамматики. Синтаксические диаграммы для описания КС-грамматик.

6. Структура компилятора. Основные функции лексического, синтаксического и контекстного анализаторов. Таблицы компиляции. Этапы генерации кода. Понятие о виртуальных машинах. Самокомпиляция и раскрутка.

7. БД и СУБД. Основные функции СУБД. Многоуровневая архитектура современных СУБД.

8. Понятие модели данных (МД). Основные компоненты МД. Традиционные МД. Отличительные особенности семантических МД.

9. Понятие модели информационной системы (ИС). Статическая, динамическая и функциональная модели ИС; связь между ними; относительная важность. Концептуальная модель, модель спецификации и модель реализации; различия в интерпретации. Понятие метамодели.

10. Язык UML, определение и назначение. Обзор основных диаграмм языка. Возможности их применения на различных этапах жизненного цикла информационной системы.

3. Защита информации

1. Информационная безопасность в системе национальной безопасности Российской Федерации. Система обеспечения информационной безопасности России.

2. Основные требования о защите информации ограниченного доступа, не составляющей государственную тайну, установленные ФСТЭК России для объектов ГИС, информационных систем управления производством, ЗО КИИ, АСУ ТП, ИСПДн, оборудования с ЧПУ.

3. Общие нормативные требования по защите персональных данных.

4. Электронная цифровая подпись. ГОСТ Р 34.10-2012.

5. Реализация системы защиты операционных систем Microsoft Windows.

6. Реализация системы защиты UNIX-подобных операционных систем.

7. Вредоносные программы: классификация, основные характеристики, современные тенденции в развитии вредоносных программ.

8. Угрозы информационной безопасности программного обеспечения. Модели безопасности информационных систем.

9. Требования доверия к безопасности информационных систем: методика формирования требований, поддержание доверия к безопасности информационных систем и программных продуктов.

10. Проблемы применения моделей безопасности при построении защищенных компьютерных систем. Проблема адекватности реализации модели безопасности в реальной компьютерной системе.

Основная литература

1. Ахо А.В., Ульман Дж.Д. Теория синтаксического анализа, перевода и компиляции: в 2 т. пер. с англ. В.Н. Агафонова; под ред. В.М. Курочкина. М.: Мир, 1978.

2. Ахо А.В., Хопкрофт Д.Э., Ульман Дж.Д. Структуры данных и алгоритмы; пер. с англ. и ред. А.А. Минько. М [и др.]: Вильямс, 2010. 391 с.

3. Бочаров П.П., Печинкин А.В. Теория вероятностей и математическая статистика: учебное пособие для студентов высших учебных заведений, обучающихся по направлениям «Физика», «Прикладная математика и информатика», специальностям «Физика», «Прикладная математика». 2-е изд. М.: ФИЗМАТЛИТ, 2005. 295 с.

4. Гордеев А.В. Операционные системы: Учеб. для студентов вузов, обучающихся по направлению подгот. бакалавров и магистров и направлению подгот. дипломир. специалистов «Информатика и вычислительная техника». 2-е изд. СПб. [и др.]: Питер, 2007. 415 с.

5. Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации: учебное пособие для студентов вузов, обучающихся по специальностям 090102 «Компьютерная безопасность», 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем», 090106 «Информационная безопасность телекоммуникационных систем» ред.: А.П. Зайцев, -4-е изд., испр. и доп. М.: Горячая линия - Телеком, 2012, ISBN 978-5-9912-0084-4. 616.

6. Камаев В.А., Костерин В.В. Технологии программирования: учеб. для студентов вузов, обучающихся по направлению подгот. специалистов «Информатика и вычислительная техника». 2-е изд., перераб. и доп. М: Высшая школа, 2006. 453 с.

7. Королев Л.Н. Структуры ЭВМ и их математическое обеспечение: [Учеб. пособие для вузов по спец. «Прикладная математика»] 2-е изд., перераб. и доп. М: Наука, 1978. 351 с.

8. Крупский В.Н., Плиско В.Е. Теория алгоритмов: учебное пособие для студентов высших учебных заведений, обучающихся по направлениям «Информатика и вычислительная техника», «Информационные системы и технологии». М: Академия, 2009. 205 с.

9. Ложников П.С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft: практикум / П.С. Ложников, Е.М. Михайлов. 3-е изд. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. 263 с. ISBN 978-5-4497-0666-9. Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт].

10. Майстренко В.А. Современные радиоэлектронные средства и технологии информационной безопасности: монография /В.А. Майстренко, А.А. Соловьев, М.Ю. Пляскин, А.И. Тихонов. Омск: Омский государственный технический университет, 2017. 356 с. ISBN 978-5-8149-2554-1. Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт].

10. Пратт Т., Зелковиц М. Языки программирования: Разработка и реализация: [Пер. с англ.] 4-е изд. М. [и др.]: Питер, 2002. 688 с.

11. Топорков В.В. Модели распределенных вычислений. М.: Физматлит, 2004. 320 с.

12. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: учебно-методическое пособие. Саратов: Вузовское образование, 2018. 218 с. ISBN 978-5-4487-0297-6. Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт].

13. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных: учебник для высших учебных заведений; под ред. А.Д. Хомоненко. 5-е изд., доп. М: Бином-Пресс; СПб.: Корона принт, 2006. 736 с.

14. Яблонский С.В. Введение в дискретную математику: учебное пособие для студентов вузов, обучающихся по специальности «Прикладная математика», изд. 6-е, стер. М: Высшая школа, 2010. 384 с.

Дополнительная литература

1. Алексеев В.Б., Ложкин С.А. Элементы теории графов, схем и автоматов: Учеб. пособие по курсам «Дискретная математика» и «Основы кибернетики» / МГУ им. М.В. Ломоносова. Фак. вычисл. математики и кибернетики. М., 2000. 60 с.

2. Верников Б.М. Элементы теории графов: учебное пособие для студентов, обучающихся по специальностям 351400 «Прикладная информатика (в экономике)» и 010300 «Математика. Компьютерные науки». Екатеринбург: Изд-во Уральского ун-та, 2005. 191 с.

3. Винокуров Н.А., Ворожцов А.В. Практика и теория программирования: учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки «Прикладные математика и физика»: в 2 кн. М.: Физматкнига, 2008.

4. Воеводин В.В. Математические модели и методы в параллельных процессах. М.: Наука, 1986. 296 с.

5. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи; пер. с англ. Е.В. Левнера, М. А. Фрумкина. М.: Мир, 1982. 416 с.

6. Девис У. Операционные системы: Функциональный подход; пер. с англ. В.В. Фролова. М.: Мир, 1980. 436 с.

7. Ездаков А.Л. Функциональное и логическое программирование: учебное пособие. 2-е изд. М: БИНОМ. Лаборатория знаний, 2011. 118 с.

8. Замятина Е.Б. Распределенные алгоритмы: учебно-методическое пособие. Пермь: Пермский гос. ун-т, 2007. 91 с.

9. Катков В.Л., Любимский Э.З. Программирование: Учеб. пособие для вузов по спец. 01.02 «Прикладная математика». Минск: Вышэйш. шк., 1992. 295 с.

10. Котов В.Е., Сабельфельд В.К. Теория схем программ. М.: Наука, 1991. 247 с.

11. Кузин А.В., Левонисова С.В. Базы данных: учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки «Информатика и вычислительная техника». 5-е изд., испр. М: Академия, 2012. 314 с.

12. Мендельсон Э. Введение в математическую логику = Introduction to mathematical logic: [исчисление высказываний, теории первого порядка, формальная арифметика, аксиоматическая теория множеств, эффективная вычислимость]; под ред. С.И. Адяна; пер. с англ. Ф.А. Кабакова, изд. 4-е. М: URSS, 2010. 319 с.

13. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации: учебник для студентов высших учебных заведений, обучающихся

по специальности «Прикладная информатика в экономике»; под ред. А.П. Пятибратова. 4-е изд., доп. и перераб. М: Финансы и статистика, 2008. 733 с.

14. Соколов А.П. Системы программирования: теория, методы, алгоритмы: учеб. пособие для студентов, обучающихся по направлению 654600 Информатика и вычисл. техника. М.: Финансы и статистика, 2004 (ОАО Тип. Новости). 319 с.

15. Справочная книга по математической логике: В 4-х ч.; под ред. Дж. Барвайса; пер. с англ. С.С. Гончарова и др. М.: Наука, 1982. 392 с.

16. Таненбаум Э. Современные операционные системы; пер. с англ. Н. Вильчинский, А. Лашкевич. 3-е изд. М. [и др.]: Питер, 2011. 1115 с.

17. Тюрин С.Ф., Аляев Ю.А. Дискретная математика: практическая дискретная математика и математическая логика: учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки дипломированных специалистов 210440 Телекоммуникации. М: Финансы и статистика: ИНФРА-М., 2010. 382 с.

18. Хоггер К. Введение в логическое программирование; пер. с англ. М.В. Захарьящева; под ред. Ю.И. Янова. М.: Мир, 1988. 348 с.

19. Безопасность ИТ: [Криптографические основы безопасности. Основы информационной безопасности. Протоколы безопасного сетевого взаимодействия. Стандарты информационной безопасности]/Интернет-Университет информационных технологий. М.: Новый диск, 2006. 1.

Составитель программы: старший преподаватель А.Н. Рабчевский.

Программа одобрена Ученым советом механико-математического факультета Пермского государственного национального исследовательского университета.