УТВЕРЖДАЮ
Проректор по науке
_____ В.В. Кружаев
«__» _____ 2014 г.

ПРОГРАММА

вступительных испытаний в аспирантуру по направлению подготовки

10.06.01 – Информационная безопасность

Екатеринбург

2014

Содержание

1. Назначение и область применения

Настоящая программа вступительного экзамена в аспирантуру по специальности 05.13.19 - "Методы и системы защиты информации и информационной безопасности" отражает современное состояние данного научно-технического направления и включает его важнейшие разделы, знание которых необходимо высококвалифицированному специалисту.

Экзаменующийся должен показать высокий уровень теоретической и профессиональной подготовки, знание основ теории, методов и средств защиты информации в современных системах ее обработки, путей и способов организации защиты с учетом текущего состояния и перспектив информатизации общества.

2. Содержание программы

В программе отражено содержание следующих вузовских дисциплин:

Алгебра,

Линейная алгебра и геометрия,

Общая алгебра,

Математический анализ,

Дифференциальные уравнения,

Теория вероятностей и математическая статистика,

Математическая логика и теория алгоритмов,

Теория графов,

Комбинаторные алгоритмы,

Теория кодирования,

Криптография,

Теоретические основы информационной безопасности,

Программно-аппаратные средства обеспечения информационной безопасности,

Организационно-правовое обеспечение информационной безопасности,

Технические средства защиты информации,

Защита информации в вычислительных сетях,

Защита информации в базах данных.

3. Вопросы для вступительного испытания

1. Теорема о существовании и единственности НОД двух многочленов.
2. Теорема о размерности пространства решений однородной системы линейных уравнений.
3. Теорема о размерности суммы двух подпространств.
4. Теорема о ранге матрицы.

5. Теорема о размерности пространства решений однородной системы линейных уравнений.
6. Критерий Сильвестра положительной определенности вещественной квадратичной формы.
7. Теорема о связи собственных значений линейного преобразования с корнями его характеристического многочлена.
8. Теорема о связи размерностей ядра и образа линейного отображения.
9. Теорема об ортогонализации линейно независимой последовательности элементов евклидова пространства.
10. Нормальные делители и факторгруппы, первая теорема о гомоморфизмах для групп.
11. Непрерывные функции. Теорема Больцано–Коши о промежуточных значениях для функций, непрерывных на отрезке. Теоремы Вейерштрасса о функциях, непрерывных на отрезке (или, более обще, на ограниченном замкнутом множестве).
12. Теоремы Ролля и Лагранжа для дифференцируемых функций. Формула Тейлора с остаточным членом в форме Лагранжа.
13. Определенный интеграл Римана по отрезку. Теорема существования определенного интеграла от непрерывной функции. Свойства интеграла с переменным верхним пределом: непрерывность и дифференцируемость. Формула Ньютона–Лейбница.
14. Степенные ряды на числовой прямой и в комплексной плоскости. Круг и радиус сходимости степенного ряда; вычисление радиуса сходимости степенного ряда. Бесконечная дифференцируемость суммы степенного ряда.
15. Дифференцируемость сложной функции от нескольких переменных; производная по направлению; градиент.
16. Теорема об общем решении линейного однородного дифференциального уравнения с постоянными коэффициентами (с доказательством для случая простых корней).
17. Схема независимых испытаний. Формула Бернулли. Теорема Пуассона.
18. Математическое ожидание случайной величины и его свойства.
19. Закон больших чисел (неравенство Чебышева, теоремы Чебышева, Маркова и Бернулли).
20. Представление булевых функций формулами алгебры высказываний и многочленами Жегалкина.
21. Замкнутые классы булевых функций, критерий полноты для булевых функций.
22. Задача о минимальном остове и алгоритм Борувки-Краскала.
23. Алгоритм Дейкстры нахождения кратчайших расстояний от выделенной вершины до остальных вершин графа.
24. Линейные коды, порождающая матрица, граница Синглтона, граница Плоткина.
25. Контрольная матрица, код Хэмминга, характеризация минимального расстояния в терминах контрольной матрицы, граница Гильберта-Варшамова.
26. Циклические коды. Коды, исправляющие пакеты ошибок, граница Рейджера, алгоритм исправления пакетов ошибок.
27. Основные параметры кодов, исправляющих ошибки: длина, скорость, минимальное расстояние. Связь между минимальным расстоянием и корректирующими возможностями кода. Граница Хэмминга.

28. Шифры замены и перестановки (общие определения и конкретные примеры). Абсолютно стойкий шифр Вернама.
29. Симметричные (одноключевые) криптосистемы. Основные режимы шифрования длинных сообщений.
30. Криптосистема RSA.
31. Свойства информации как объекта защиты
32. Стратегии информационной защиты и модели, построенные на их основе.
33. Классификация и определение технических каналов утечки информации. Основные средства и методы защиты акустической информации от утечки по техническим каналам. Организационные и инструментальные методы обнаружения средств негласного подслушивания.
34. Принципы действия сигнализационных датчиков инфракрасного и радиотехнического типов. Построение чувствительных элементов и трактов обработки тревожной информации. Требования к размещению датчиков на объекте.
35. Общая характеристика систем управления физическим и логическим доступом на объекты информатизации. Парольные системы. Физические носители ключевой информации. Биометрические системы. Сравнительная характеристика методов идентификации и аутентификации.
36. Принципы защиты компьютерной информации, хранимой на внешних машинных носителях. Порядок регистрации, выдачи, хранения, передачи и уничтожения машинных носителей с конфиденциальными данными. Аппаратно-программные средства для гарантированного удаления информации. Способы реставрации информации на магнитных носителях.
37. Основные свойства файловой системы NTFS. Понятие об MFT. Структура записи в MFT. Организация резидентных и нерезидентных файлов в NTFS. Понятие об EFS. Структура зашифрованного файла.
38. Реализация защиты компьютерной информации в файловых системах Linux. Особенности файловых систем EXT*FS. Структура метаданных и их размещение на дисковом пространстве. Права доступа. Работа с объектами файловой системы.
39. Аудит безопасности компьютерных систем. Цели, стандарты и подходы. Инструментальные средства аудита безопасности компьютерных систем, их возможности и недостатки.
40. Применение специализированных программных средств защиты информации (СЗИ), их достоинства и недостатки. Требования к специализированным средствам защиты информации от НСД. Организация виртуальных защищенных логических дисков. Контроль «технологического» мусора. Механизмы организации контроля доступа до загрузки операционной системы (ОС). Механизмы доверенной загрузки ОС, реализованные в СЗИ.
41. Реализация политики разграничения доступа в операционных системах MS Windows 2000, XP. Реализация механизмов идентификации и аутентификации в ОС MS Windows 2000, XP. Хранение парольной информации в операционной системе.
42. Классификация сетевых атак. Сканирование сети и разведка ее топологии. Возможности злоумышленников по перехвату и перенаправлению информации, передаваемой в компьютерных сетях. Методы вредоносного блокирования сетевых

узлов и каналов связи.

43. Понятия о межсетевом экранировании. Политика сетевой безопасности. Критерии фильтрации пакетов. Основные схемы защиты компьютерной информации на основе межсетевых экранов.
44. Организация VPN-сетей. Задачи, решаемые VPN. Туннелирование в VPN. Протоколы и средства организации VPN на сетевом уровне. Назначение, область применения, аутентификация и шифрование данных в протоколах SKIP и IPSec.
45. Протоколы PPTP, SSL. Назначение, область применения, аутентификация и шифрование данных. Электронные сертификаты. Понятие инфраструктуры открытых ключей. Стандарт X.509.
46. Условия правомерного использования программ для ЭВМ и баз данных. Ответственность за нарушение норм авторского права.
47. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Характеристика объективной стороны преступлений, предусмотренных ст. 272-274 УК РФ. Определение ключевых понятий: вредоносное удаление, копирование, блокирование и модификация компьютерной информации, виды нарушений работы ЭВМ. Субъекты преступлений. Санкции за совершение преступных деяний.
48. Типичные конфликтные ситуации, возникающие между администратором компьютерной сети и руководством организации по поводу обеспечения информационной безопасности, и методы их разрешения.
49. Типичные конфликтные ситуации, возникающие между администратором компьютерной сети и пользователями ЭВМ по поводу обеспечения информационной безопасности, и варианты их разрешения.
50. Порядок взаимодействия оператора связи и администрации компьютерных сетей с представителями правоохранительных органов по вопросам, предусмотренным Федеральным законодательством.
51. Определение и классификация вредоносных программ для ЭВМ. Деструктивные возможности компьютерных программ. Программные методы вредоносного удаления, копирования, блокирования, модификации компьютерной информации и нарушений работы ЭВМ.
52. Организационные и программные средства и методы антивирусной защиты, оценка их эффективности.
53. Реализация механизмов защиты компьютерной информации на уровне клиентских приложений (на примерах текстового процессора Microsoft Word и браузера Microsoft Internet Explorer).
54. Понятие и классификация (таксонометрия) угроз безопасности компьютерной информации. ГОСТ Р 51275-99. Потери и ущерб от реализации угроз. Понятие политики и моделей безопасности в компьютерных системах.

4. Критерии оценки знаний претендентов на поступление в аспирантуру по направлению подготовки 10.06.01 – Информационная безопасность

Оценка ответов претендентов на поступление в аспирантуру по данному направлению производится по пяти балльной шкале и выставляется согласно критериям, приведенным в таблице.

Критерии оценки ответов претендентов при поступлении в аспирантуру

Оценка	Критерии
Отлично	1. Ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. 2. Демонстрируются глубокие знания по дисциплине. 3. Делаются обоснованные выводы. 4. Ответ самостоятельный, при ответе использованы знания, приобретённые ранее.
Хорошо	1. Ответы на поставленные вопросы излагаются систематизировано и последовательно. 2. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. 3. Материал излагается уверенно, в основном правильно даны все определения и понятия. 4. Допущены небольшие неточности при выводах и использовании терминов.
Удовлетворительно	1. Допускаются нарушения в последовательности изложения при ответе. 2. Демонстрируются поверхностные знания дисциплины. 3. Имеются затруднения с выводами. 4. Определения и понятия даны не чётко.
Неудовлетворительно	1. Материал излагается непоследовательно, сбивчиво, не представляет определённой системы знаний по дисциплине. 2. Не даны ответы на дополнительные вопросы комиссии. 3. Допущены грубые ошибки в определениях и понятиях.

5. Список рекомендуемой литературы

Основная литература

1. Асанов М.О., Баранский В.А., Расин В.В. Дискретная математика: графы, матроиды, алгоритмы. – СПб.: Издательство «Лань», 2010. – 368 с.
2. Бакланов В.В., Пономарев М.Э. Опасная компьютерная информация: учеб. пособие. — Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2007. — 146 с.
3. Бакланов В. В. Введение в информационную безопасность. Направления информационной защиты: Учебное пособие / В. В. Бакланов. – Екатеринбург: ГОУ ВПО УрГУ, 2006. - 236 с.
4. Бакланов В.В. Защитные механизмы операционной системы Linux: учебное пособие. – Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2009. – 278 с.
5. Баранский В.А., Кабанов В.В. Общая алгебра и ее приложения. – Екатеринбург: Изд-во Урал. Ун-та, 2003. – 244 с.
6. Вентцель Е.С. Теория вероятностей. М.: Высшая школа, 2002.
7. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во Урал. Ун-та, 2003. – 328 с.

8. Духан Е.И. Применение программно-аппаратных средств защиты компьютерной информации: учеб. пособие / Е.И. Духан, Н.И. Синадский, Д.А. Хорьков. – Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2008. — 182 с.
9. Зайцев А. П. Технические средства и методы защиты информации: Учебное пособие для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2009. – 616 с.
10. Ильин В.А., Садовничий В.А., Сендов Б.Х. Математический анализ: в 2-х ч. М.: Изд-во Московского ун-та, 2007(2006, 2004). Ч.1,2.
11. Кострикин А.И. Введение в алгебру. М.: МЦНМО, 2009.
12. Курош А.Г. Курс высшей алгебры. 12-е изд., стер. СПб.: Лань, 2003.
13. Кудрявцев Л.Д. Краткий курс математического анализа: в 2-х тт. М.: ФИЗМАТЛИТ, 2005(2003, 2002). Т.1,2.
14. Расторгуев С. П. Основы информационной безопасности: Учебное пособие для студентов высших учебных заведений / С. П. Расторгуев. – М.: Академия, 2007. – 192 с.
15. Смарт Н. Криптография. – М.: Техносфера, 2005.
16. Фаддеев Д.К. Лекции по алгебре. 3-е изд., стер. СПб.: Лань, 2004.
17. Эльсгольц Л.Э. Обыкновенные дифференциальные уравнения. СПб.: Лань, 2002.

Дополнительная литература

1. Андрончик А. Н. и др. Защита информации в компьютерных сетях. Практический курс: Учебное пособие /А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; Под ред. Н. И. Синадского. — Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2008. — 248 с.
2. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс: Учебное пособие. — М.: Гелиос АРВ, 2002. — 368 с.
3. Курош А.Г. Лекции по общей алгебре. Изд. 2-е, стер. СПб.: Лань, 2007.

4. Понтрягин Л.С. Обыкновенные дифференциальные уравнения. М.; Ижевск: РХД, 2001.
5. Севастьянов В.А. Курс теории вероятностей и математической статистики. М.:Наука, 1982.
6. Синадский Н. И. Анализ и восстановление данных на носителях с файловой системой NTFS: учеб. пособие. – Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2007. – 136 с.
7. Тутубалин В.Н. Теория вероятностей. М.: Академия, 2008.
8. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления: в 3-х тт. М.: ФИЗМАТЛИТ, 2008(2007, 2006). Т.1-3.
9.Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления : в 3-х тт. СПб. [и др.]: Лань, 2009. Т.1-3.
10. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов : в 3 т. / А. А. Хорев – М.: НПЦ «Аналитика», 2008.
11. Шнайер Б. Прикладная криптография. – М., Триумф: 2003.

6. Рекомендуемые Интернет-ресурсы www.academy.fsb.ru

Программу вступительного испытания в аспирантуру по направлению подготовки 10.06.01 – Информационная безопасность разработал:

Профессор кафедры алгебры и дискретной математики, доктор физ.-мат. наук, профессор В.А. Баранский

Лист согласования

Директор Института математики и компьютерных наук — М.О. Асанов

Заведующий кафедрой алгебры и дискретной математики — М.В. Волков

Профессор кафедры алгебры и дискретной математики — В.А. Баранский