Министерство науки и высшего образования Российской Федерации
ФГАОУ ВО «Волгоградский государственный университет»

УТВЕРЖДЕНО
Ученым советом
Института приоритетных технологий
«19» декабря 2023 г.
протокол № 12
Директор института
_____Запороцкова И.В.

УТВЕРЖДАЮ
Председатель
приемной комиссии
_____А.Э. Калинина
«18» января 2024 г.

УТВЕРЖДЕНО
Ученым советом
Института математики и информационных технологий
«25» декабря 2023 г.
протокол № 12
Директор института
_____Лосев А.Г.

ПРОГРАММА

вступительного испытания в аспирантуру

по группе научных специальностей

2.3 - Информационные технологии и телекоммуникации

Волгоград 2023 г.

Цель и задачи вступительного экзамена

Программы вступительных испытаний при приеме на обучение по программам подготовки научных и научно-педагогических кадров в аспирантуре формируются на основе федеральных государственных образовательных стандартов высшего образования по программам специалитета или магистратуры.

Билет вступительного экзамена включает **три вопроса**, взятых из разных разделов настоящей Программы.

Вступительные испытания в аспирантуру проводятся в форме устного комплексного экзамена.

Цель экзамена – определить готовность и возможность лица, поступающего в аспирантуру, освоить выбранную программу.

Основные задачи экзамена:

• проверка уровня знаний претендента;

• определение склонности к научно-исследовательской деятельности;

• выяснение мотивов поступления в аспирантуру;

• определение уровня научных интересов;

• определение уровня научно-технической эрудиции претендента.

Ориентировочная продолжительность экзамена – 45 мин.

В ходе вступительных испытаний поступающий должен показать:

• знание теоретических основ дисциплин бакалавриата (специалитета), магистратуры по соответствующему направлению;

• владение специальной профессиональной терминологией и лексикой;

• умение оперировать ссылками на соответствующие положения в учебной и научной литературе;

• владение культурой мышления, способность в письменной и устной речи правильно оформлять его результаты;

• умение поставить цель и сформулировать задачи, связанные с реализацией профессиональных функций.

Результаты вступительных испытаний оцениваются по **пятибалльной** шкале.

Оценка определяется как средний балл, выставленный экзаменаторами во время экзамена.

Критерии оценки результатов комплексного экзамена в аспирантуру

5 (Отлично)

Полный безошибочный ответ, в том числе на дополнительные вопросы членов экзаменационной комиссии. Поступающий должен правильно определять понятия и категории, выявлять основные тенденции и противоречия, свободно ориентироваться в теоретическом и практическом материале.

4 (Хорошо)

Правильные и достаточно полные, не содержащие ошибок и упущений ответы. Оценка может быть снижена в случае затруднений студента при ответе на дополнительные вопросы членов экзаменационной комиссии. При ответе допущены отдельные несущественные ошибки.

3 (Удовлетворительно)

Недостаточно полный объем ответов, наличие ошибок и некоторых пробелов в знаниях.

2 (Неудовлетворительно)

Неполный объем ответов, наличие ошибок и пробелов в знаниях или отсутствие необходимых знаний.

При выставлении итоговой оценки на вступительном экзамене в аспирантуру по специальной дисциплине учитываются результаты собеседования по тематике представленного реферата, который отражает собственные научные интересы поступающего и предполагаемое направление научных исследований в процессе обучения в аспирантуре.

Программа вступительного экзамена в аспирантуру

по научной специальности

2.3.6 Методы и системы защиты информации, информационная безопасность

1. Задачи помехоустойчивого кодирования. Границы для параметров кодов. Методы декодирования при применении линейных кодов.
2. Код Хемминга. Методы построения новых кодов. Тождества Мак-Уильямс. Циклические коды. Коды БЧХ, исправляющие заданное число ошибок.
3. Классификация каналов связи. Пропускная способность. Вычисление пропускной способности для дискретного канала без памяти.
4. Прямая и обратная теоремы Шеннона для двоичного симметричного канала. Теоремы кодирования для дискретных каналов без памяти.
5. Жизненный цикл программного обеспечения, Характеристика этапов жизненного цикла программного обеспечения.
6. Качество и надежность программного обеспечения, Безопасность программного обеспечения, Методы защиты программ и данных в языках программирования высокого уровня.
7. Документирование проектирования, Понятия отладки и тестирования, Верификация и тестирование, Стратегия проектирования тестов. Принципы отладки, Автономное тестирование. Комплексное тестирование, Тестирование программы на этапе кодирования, Отладка программы.
8. Основные определения. Операция перестановки. Операция подстановки. Роторные машины.
9. Перестановка. Гаммирование. Генераторы псевдослучайной последовательности. Регистр сдвига с линейной обратной связью. Аппаратный генератор случайных чисел.
10. Симметричные криптосистемы. Блочные шифры. Сеть Фейстеля. SP-сеть.
11. Ассиметричные криптосистемы. Схема Эль-Гамаля. Криптосистема, основанная на проблеме Диффи-Хеллмана.

12. Ассиметричные криптосистемы. Криптосистема RSA. Криптосистемы Меркля — Хеллмана и Хора — Ривеста.
13. Криптосистемы над группой точек эллиптической кривой. Построение группы точек эллиптической кривой.
14. Понятие логической схемы как устройства, преобразующего электрические сигналы двух уровней. Вентили как простейшие логические схемы с одним или двумя входами и одним выходом. 2.
15. Реализация логических функций с помощью вентилей. Функции одной переменной. Вентиль НЕ: условное обозначение, таблица истинности, булева функция и название выполняемой операции. Функции двух переменных. Вентили И, ИЛИ, И-НЕ, ИЛИ-НЕ, ИСКЛЮЧАЮЩЕЕ ИЛИ, ИСКЛЮЧАЮЩЕЕ ИЛИ-НЕ: условные обозначения, таблицы истинности, булевы функции и названия выполняемых операций.
16. Логические схемы с произвольным числом m входов и одним выходом как устройства для реализации логических функций от m переменных. Алгоритм построения таких схем из вентилей И, ИЛИ, НЕ. Понятие о двухуровневой технологии реализации логических функций. Пример: схемная реализация «функции большинства» для трех переменных.
17. Дешифратор базового типа. Принцип работы базового дешифратора и его применение для перевода чисел из двоичной системы в десятичную. Реализация логических функций с помощью базовых дешифраторов. Условное обозначение, таблица истинности, булевы функции и схемное построение базового дешифратора 3:8. Его применение для реализации «функции большинства» от трех переменных.
18. Эталонная модель взаимодействия открытых систем Open Systems Interconnection. Особенности эталонной модели. Прикладной уровень. Уровень представления. Сеансовый уровень. Транспортный уровень. Сетевой уровень. Канальный уровень. Физический уровень. Стек протоколов TCP/IP. Уровень доступа к сети. Межсетевой уровень модели TCP/IP. Транспортный уровень. Стек TCP/IP.

19. Слабости протоколов Address Resolution Protocol (ARP), Internet Protocol v4 и v6 (IP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), Dynamic Host Configuration Protocol (DHCP), Domain Name Server (DNS). Методы защиты.
20. Классификация виртуальный частный сетей (Virtual Private Network). Доверенные и защищенные сети. Реализации. Схемы подключения. Протоколы Point-To-Point Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), L2TP/IPSEC.
21. Протокол IPSEC. Порядок обработки сетевого трафика в протоколе IPSEC. Протоколы AH и ESP. Протокол IKE1/IKE2. Рекомендуемые режимы работы.
22. Логическая («виртуальная») локальная компьютерная сеть Virtual Local Area Network (VLAN). Access и Trunk-порты. Номера VLAN. Проблемы безопасности VLAN.
23. Технология Port-Security. Статические и динамические подход формирования БД. Способы реакции. Технологии Direct ARP Inspection/Protection, DHCP Snooping.
24. Протокол SSL/TLS. Назначение. Версии. Алгоритм создания подключения. Режимы работы. Проблемы безопасности.
25. Сети Петри. Основные свойства сетей Петри. Виды сетей Петри. Примирение сетей Петри к решению задач обеспечения информационной безопасности.
26. Моделирование случайных процессов. Поток событий. Простейший поток и его свойства. Марковский случайный процесс. Классификация марковских процессов. Расчет марковской цепи с дискретным временем. Пуассоновские потоки событий и непрерывные марковские цепи. Предельные вероятности состояний для марковской цепи.
27. Основные положения теории нечетких множеств. Операции на нечетких множествах. Нечеткие отношения. Нечеткие системы в информационной

безопасности. Этапы нечеткого логического вывода. Построение базы нечетких правил.

28. Типичный сценарий действий нарушителя. Сбор информации. Реализация атаки. Завершение атаки.
29. Средства обнаружения компьютерных атак. Признаки атак. Повтор определенных событий. Неправильные команды. Использование уязвимостей. Несоответствующие параметры сетевого трафика. Непредвиденные атрибуты. Необъяснимые проблемы. Дополнительные признаки.
30. Источники информации об атаках. Технологии обнаружения атак. Обнаружение аномальной активности. Обнаружение злоупотреблений.

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

1. Басалова Г.В. Основы криптографии // Интуит НОУ, 2016
2. Бехроуз А. Фороузан Математика криптографии и теория шифрования // Интуит НОУ, 2016
3. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft // Интуит НОУ, 2016
4. А.П. Курило Основы управления информационной безопасностью М.: Горячая линия-Телеком, 2012
5. Милославская. Н.Г. Вопросы управление информационной безопасностью. Москва: Горячая линия-Телеком, 2013.
6. Приказ Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
7. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
8. О.И.Шелухин, А.Н.Руднев, А.В.Савелов Системы обнаружения вторжений в компьютерные сети // Учебное пособие. МТУСИ, Москва, 2015 г, 97 стр.
9. Сакалема Д.Ж., Филинова А.С., Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) // Учебное пособие для вузов / М.: Горячая линия–Телеком, 2015. – 220 с.

10. Мэйволд Э.Безопасность сетей. Национальный Открытый Университет «ИНТУИТ» Национальный Открытый Университет «ИНТУИТ» – 2016 г. – 572 с.
11. Платунова, С.М. Построение корпоративной сети с применением коммутационного оборудования и настройкой безопасности. Учебное пособие по дисциплине «Корпоративные сети». [Электронный ресурс] — Электрон. дан. — СПб.: НИУ ИТМО, 2012. — 85 с.
12. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. - М.: ГТК - 1992 г. - 13с.
13. Разработка и эксплуатация удаленных баз данных. Учебник. Фуфаев Э.В., Фуфаев Д.Э. Academia, 2014, 256 с.
14. Романьков В.А. Введение в криптографию. Курс лекций. Серия: Высшее образование. М.: Форум, 2012.
Ященко В.В. Введение в криптографию. МЦНМО, 2012 г
15. Сети и системы передачи информации. Телекоммуникационные сети. Учебник и практикум Самуйлов К., Шалимов И., Кулябов Д. и др. Юрайт, 2016, 364 с.
16. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками, Горячая линия - Телеком, 2013
17. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. Олифер В. Г., Олифер Н. А. СПб. : Питер, 2012, 944 с., МО РФ
18. Руководящий документ. ФСТЭК. Режим доступа: http://fstec.ru/component/tags/tag/7- rukovodyashchij-dokument
19. Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения информационной безопасности // Проспект, 2015

Содержание вступительного испытания в аспирантуру по научной специальности 2.3.1 "Системный анализ, управление, обработка информации"

1. Понятия о системном подходе, системном анализе. Выделение системы из среды, определение системы.

2. Системы и закономерности их функционирования и развития. Свойства системы: целостность и членимость, связность, структура, организация, интегрированные качества.

3. Модели систем: статические, динамические, концептуальные, топологические, информационные, логико-лингвистические и др.

4. Анализ и синтез как базовые подходы к исследованию и моделированию систем.

5. Определение и общая классификация видов информационных технологий. Модели, методы и средства сбора, хранения, коммуникации и обработки информации с использованием компьютеров.

6. Формы представления и кодирование информации. Способы кодирования чисел: формат с плавающей точкой, с фиксированной точкой. Кодирование символьных данных.

7. Обобщенная структура современных вычислительных систем: основные компоненты, их назначение, принцип работы.

8. Микропроцессоры (МП): понятие, классификация, обобщенная структура, принцип работы. Система команд МП. Отличия микропроцессора и микроконтроллера.

9. Системное и прикладное программное обеспечение. Операционные системы, их функции. Виды операционных систем. Многозадачность в операционных системах.

10. Алгоритм, его свойства, методы разработки. Этапы решения инженерных задач с использованием компьютерной техники.

11. Языки программирования: классификация. Критерии выбора языка программирования для решения конкретной задачи. Понятие интегрированной среды разработки (IDE).

12. Технологии структурного, модульного, объектно-ориентированного, компонентно-ориентированного проектирования.

13. Понятие компьютерной графики. Представление графической информации в компьютере. Растровая и векторная графика. Интерфейс программирования графики OpenGL: область применения, основные особенности.

14. Понятие параллельных вычислений. Условия достижения параллелизма. Конвейерная организация вычислений. Классификация вычислительных систем. Суперкомпьютеры.

15. Топологии сети передачи данных. Характеристики топологии сети.

16. Основные интерфейсы и стандарты для параллельного программирования: MPI, OpenMP. Области применения, особенности.

17. Основные сетевые концепции. Глобальные, территориальные и локальные сети. Сетевая модель OSI. Модели взаимодействия компьютеров в сети.

18. Среда передачи данных. Преобразование сообщений в электрические сигналы, их виды и параметры. Проводные и беспроводные каналы передачи данных

19. Локальные сети. Протоколы, базовые схемы пакетов сообщений и топологии локальных сетей. Сетевое оборудование ЛВС.

20. Глобальные сети. Основные понятия и определения. Сети с коммутацией пакетов и ячеек, схемотехника и протоколы. Принципы межсетевого взаимодействия и организации пользовательского доступа. Способы защиты информации.

21. Принципы функционирования Internet, типовые информационные объекты и ресурсы.

22. Основные понятия систем баз данных. Назначение и основные компоненты систем баз данных: база данных, система управления базами данных (СУБД).

23. Программные и языковые средства СУБД, пользователи баз данных, администратор систем баз данных и его функции.

24. Проектирование баз данных. Основные этапы проектирования БД: системный анализ предметной области.

25. Понятия объект, свойства, отношения объектов, классы объектов, экземпляры объектов, идентификатор экземпляров объектов. Понятия сущность, атрибуты, связи, первичные ключи сущностей. Типы связей.

26. Построение семантической модели взаимосвязи объектов предметной области с помощью диаграмм ER-типа.

27. Логическое и физическое проектирование реляционных баз данных. Отношения, атрибуты отношений и их домены, схема отношения.

28. Структурированный язык запросов SQL. Простая выборка, выборка с использованием соединения отношений, подзапросы, коррелированные подзапросы.

29. Аксиоматическое и геометрическое определение вероятности события, свойства вероятности. Виды количественного описания поведения случайных величин всех типов.

30. Случайные величины, их законы распределения и числовые характеристики.

31. Предельные теоремы теории вероятностей (общая и частная теорема Чебышева, теорема Бернулли, центральная предельная теорема).

32. Точечное и интервальное оценивание параметров распределений случайных величин. Законы распределения и характеристики случайных процессов.

33. Транспортная задача линейного программирования: постановка задачи оптимизации перевозок, математическая модель транспортной задачи.

34. Методы решения транспортных задач, методы улучшения допустимых решений, различные постановки и модели транспортных задач, задачи с правильным и неправильным балансом.

35. Транспортная задача по критерию времени, задача о назначениях, решение задачи о назначениях.

36. Дискретное программирование: общая постановка задачи дискретного программирования, особенности методов решения задач.

37. Задачи оптимального выбора, задача о рюкзаке, постановка и эвристический метод решения.

39. Метод динамического программирования. Принцип оптимальности Беллмана. Вычислительная схема метода.

39. Задача оптимального выбора проектов, примеры решения задач оптимального выбора, задача коммивояжера, методы решения задачи коммивояжера.

40. Принятие решений в конфликтных ситуациях: основные типы конфликтных ситуаций, предмет и методы теории игр, классификация задач теории игр.

41. Антагонистические игры двух лиц с нулевой суммой, платежная матрица игры, примеры постановок игровых задач принятия решений.

42. Алгоритмы машинного обучения: обучение с учителем, обучение без учителя, обучение с подкреплением

43. Нейронные сети: виды нейронных сетей, методы обучения нейронных сетей.

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

1. Тарасенко Ф.П. Прикладной системный анализ : учебное пособие / Ф. П. Тарасенко. — М. : КНОРУС, 2010. — 224 с.
2. Информатика. Базовый курс. Учебник для ВУЗов. Под ред. С.В.Симоновича. Санкт- Петербург: Питер, 2000. – 640 с.
3. Информатика. Под ред. Н.В.Макаровой. 3-е изд. М.: Финансы и статистика. 2001. - 768 с.
4. Савельев А.Я. Основы информатики. - М.: МГТУ им. Н.Э.Баумана, 2001. – 328 с.
5. Залогова Л. А. Компьютерная графика [Электронный ресурс] : / Л. А. Залогова; [науч. ред. С. В. Русаков]. – Москва: Бином. Лаборатория знаний, 2014. – 245 с. – ISBN 978-5-9963-2374-6. – Режим доступа: http://e.lanbook.com/view/book/50554.
6. Д. Херн. Компьютерная графика и стандарт OpenGL / Д. Херн, М.Бейкер. М.: Издательский дом «Вильямс», 2005. – 1168 с. – ISBN 5-8459-0772-1.
7. Богачѐв К.Ю. Основы параллельного программирования / К.Ю.Богачев. – М.: БИНОМ. Лаборатория знаний, 2013. – 342 с., ил. – ISBN 978-5-9963-0939-9. – Точка доступа : http://e.lanbook.com/books/element.php?pl1_id=42626.

8. Модели параллельного программирования: Практическое пособие / Федотов И.Е. - М.:СОЛОН-Пр., 2017. - 392 с.: 60х88 1/8. - (Библиотека профессионала) ISBN 978-5-91359-222-4 - Режим доступа: http://znanium.com/catalog/product/858609
9. Вентцель Е.С. Теория вероятностей. М., Высшая школа, 2005.
10. Гмурман В.Е. Теория вероятностей и математическая статистика. М., Высшая школа, 2005.
11. Вентцель Е.С. Исследование операций. - М.: Высшая школа. 2007.
12. Таха Хемди А. Введение в исследование операций. - М.: Вильямс, 2007.
13. Черноруцкий И.Г. Методы принятия решений. - СПб.: БХВ, 2005.
14. Ширяев В.И. Исследование операций и численные методы оптимизации. - М.: КомКнига, 2007.
15. Карпова Т.С. Базы данных: Модели, разработка, реализация. Учебник. - СПб.: Питер, 2001.
16. Ризаев И.С., Яхина З.Т. Базы данных. Учебное пособие. - Казань: Изд-во КГТУ. 2002.
17. Дейт К. Дж. Введение в системы баз данных. - М: Вильямс, 2006.
17. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных. Учебник. - Москва : Бином,2006.
18. Конноли Т., Бегг К. Базы данных: проектирование, реализация и сопровождение. Теория и практика, 2-е изд. - М.: Из д. дом «Вильямс». 2000