**ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО КОНКУРСНОЙ ГРУППЕ
«ФРКТ КОМПЬЮТЕРНЫЕ НАУКИ И ИНФОРМАТИКА»
(ДЛЯ ПОСТУПАЮЩИХ В АСПИРАНТУРУ)**

Билет включает 2 вопроса. Первый вопрос - из раздела программы, соответствующего научной специальности, по которой поступающий намерен обучаться. Второй вопрос - по будущей диссертационной работе поступающего: тематика, имеющийся задел, наличие научного руководителя, публикаций. Могут быть также заданы вопросы по содержанию выпускной квалификационной работы (магистра, специалиста).

На подготовку дается 1 час, при этом разрешено пользоваться литературой за исключением электронных носителей. Не разрешается использование средств связи и доступа в интернет. Поступающий отвечает по билету в форме устного собеседования, в ходе которого могут быть заданы дополнительные вопросы по соответствующему разделу программы.

Раздел «Математическое моделирование, численные методы и комплексы программ»

1. Решение систем нелинейных уравнений. Метод Ньютона. Теорема о квадратичной скорости сходимости. Методы простых итераций, анализ сходимости. Метод продолжения по параметру.
2. Численное дифференцирование. Основные разностные аппроксимации первых и вторых производных. Ошибка аппроксимации, ошибка округления. Оптимальный шаг численного дифференцирования. Метод сеток для уравнения теплопроводности. Простейшие разностные схемы (явная, неявная). Аппроксимация уравнений, начальных и краевых условий. Реализация явной схемы. Счет по слоям. Реализация неявной схемы, уравнения на верхнем слое, его решение методом прогонки.
3. Численное интегрирование задачи Коши для систем ОДУ. Метод сеток, простейшие разностные схемы (Явная и неявная схемы Эйлера, схема с центральной разностью). Реализация разностных схем. Ошибка аппроксимации, критерии малости шага сетки.
4. Типичные задачи вычислительной линейной алгебры. Матричный анализ. Теория возмущений и числа обусловленности. Вычисления с конечной точностью.
5. Треугольные системы. LU-разложение. Симметричные матрицы. Ленточные матрицы. Разреженные матрицы. LDMT и LDLT разложения. Ортогональные матрицы. Матрицы Хаусхолдера и Гивенса. QR-разложение. SVD-разложение.
6. Проблема собственных значений. Хессенбергова форма и форма Шура. Теория возмущений. Устойчивый QR метод. Симметричный QR метод и SVD.
7. Выпуклая оптимизация и двойственность. Условия экстремума в гладких задачах, теорема Левитина-Милютин-Осмоловского. Двойственность в выпуклом и линейном программировании.
8. Принцип максимума Понтрягина в вариационном исчислении и оптимальном управлении.
9. Принцип Лагранжа для гладко-выпуклых задач. Принцип Лагранжа в теории оптимального управления.
10. Основные понятия и задачи статистического оценивания. Экспоненциальное и регулярное семейства распределений. Правдоподобие. Статистическая теория принятия решений.
11. Байесовский вывод. Сравнение байесовского и частотного подхода к статистическому оцениванию. Байесовская теория принятия решений. Исключение мешающих параметров. Перестановочность. Теорема де Финетти.
12. Асимптотическая нормальность апостериорного распределения. Теорема Дуба. Условия Ибрагимова и Хасьминского. Состоятельность байесовских оценок. Теорема Бернштейна фон Мизеса.

13. Линейный регрессионный анализ. Обычный и обобщенный методы наименьших квадратов. Оценивание ошибок линейной модели. Проверка гипотез о параметрах линейной модели. Доверительные интервалы.
14. Нелинейный регрессионный анализ. Основные методы непараметрической регрессии (многомерная непараметрическая регрессия, нейронные сети, радиальные базисные функции, регрессия на основе системы поддерживающих векторов, кригинг).
15. Постановка задачи снижения размерности. Линейные методы снижения размерности. Анализ главных компонент. Многомерное шкалирование.
16. Постановка задачи классификации. Байесовский классификатор. Линейные классификаторы: перцептрон. Алгоритм Розенблатта. Метод опорных векторов. Оптимальная гиперплоскость. Алгоритм построения оптимальной гиперплоскости. Оценка вероятности ошибки обобщения через число опорных векторов.
17. Теория обобщения Вапника–Червоненкиса. VC-размерность, определение, основное свойство. Верхняя оценка вероятности ошибки классификации через VC-размерность класса функций классификации.
18. Задача универсального прогнозирования в режиме онлайн: статистический подход. Калибруемость прогнозов. Алгоритм вычисления хорошо калибруемых прогнозов.
19. Элементы теории алгоритмов Машины Тьюринга, машины Поста, нормальные алгоритмы Маркова. Оценки сложности алгоритмов. NP – Задачи (алгоритмы).
20. Элементы теории языков. Конечные автоматы – автоматные грамматики, магазинные автоматы – контекстно-свободные грамматики.
21. Алгоритмы на графах. Понятие графа. Особые классы графов. Поиск на графах в ширину, в глубину. Алгоритмы поиска минимального пути.
22. Объект = данные + методы работы с ними. Абстракция как средство моделирования реальности при помощи объектов. Инкапсуляция. Модификация и оптимизация программ при помощи инкапсуляции. Наследование. Повторное использование кода. Полиморфизм как средство обеспечения расширяемости программ. Понятие интерфейса как альтернативного средства обеспечения полиморфизма.
23. Динамические массивы, списки и их сравнение. Очередь и стек. Понятие отображения (map). Реализация отображений через бинарные деревья и хэш-таблицы. Понятия динамических объектов и кучи (heap). Базовые операции работы с кучей. Сборка мусора.
24. СУБД. Логическая и физическая структура данных. Средства обеспечения целостности данных. Транзакции. Реляционная модель данных. Нормализация данных. ER – диаграммы. Язык SQL. Хранилища данных. Сравнение с операционными БД. Денормализация. Многомерная модель данных. OLAP. Витрины данных. Их использование в качестве промежуточного слоя в трехуровневой архитектуре.
25. Понятие архитектуры распределенных вычислительных систем. Компьютерные сети. Семиуровневая модель взаимодействия открытых систем (OSI Seven – Layer Model). Концепция клиент-сервер. Примеры ее применения.

Раздел «Теоретическая информатика, кибернетика»

1. Общие принципы моделирования процессов мышления человека и человеко-машинного общения. Машинное представление знаний и данных. Методы хранения, поиска и обработки данных, методы естественно-языкового человеко-машинного общения
2. Передача информации. Модель системы связи и роль каждого из блоков. Шенноновские меры информации: собственная информация, энтропия, взаимная информация.
3. Статистические источники с памятью и без памяти. Энтропия стационарного источника. Предельные средняя и условная энтропии.
4. Кодирование источника информации. Теоремы Шеннона для источника. Разделимые и неразделимые коды. Префиксный код. Теорема Мак-Миллана. Неравенство Крафта.

5. Коды Шеннона, Фано, Хаффмена. Универсальное кодирование: алгоритмы Лемпела-Зива-Велча, алгоритм Лемпела-Зива. Арифметическое кодирование.
6. Кодирование для канала: Классификация каналов. Лемма об обработке информации и граница Фано. Пропускная способность канала. Симметричный канал без памяти, его параметры и характеристики. Вычисление пропускной способности каналов, учет симметрии по входам и выходам.
7. Декодирование как разделение всей области сигналов на выходе канала на отдельные подобласти. Декодирование с отказом решений и без отказов. Ошибки декодирования.
8. Прямая и обратная теоремы Шеннона. Экспонента вероятности ошибки для бинарного симметричного канала без памяти.
9. Непрерывные источники и непрерывные каналы. Теорема Котельникова.
10. Конечные поля, векторные пространства. Группы, кольца и поля. Кольца многочленов. Алгоритм Евклида.
11. Блочные коды. Границы Синглтона, Плоткина, Бассальго—Элайеса, Хэмминга, Варшамова—Гилберта.
12. Циклические коды. Систематическая форма порождающей и проверочной матриц.
13. Коды Боуза—Чоудхури—Хоквингема (БЧХ). Коды Рида—Соломона (РС). Алгебраическое декодирование кодов Рида-Соломона.
14. Сверточные коды. Алгоритм Витерби. Турбо коды и коды с низкой плотностью проверок на четность.
15. Ранговые коды. Матричное и векторное представление. Граница Синглтона. Алгоритмы декодирования.
16. Информация как предмет защиты. Особенности информации как предмета защиты. Сценарии обмена информацией между двумя сторонами: обеспечение конфиденциальности; обеспечение целостности (хэш-функции);
17. Обеспечение аутентификации сообщений и идентификации сторон (протоколы); обеспечение невозможности отказа от авторства передающей стороной и невозможности подделки приемной стороной (цифровая подпись, хэш-функции).
18. Сравнения по модулю. Малая теорема Ферма. Функция Эйлера. Китайская теорема об остатках.
19. Сложность алгоритмов сложения, умножения, возведения в целую степень.
20. Криптография и криптоанализ. Ключи шифрования. Допущения при криптоанализе. Криптостойкость системы защиты информации.

Раздел «Искусственный интеллект и машинное обучение»

1. Определение искусственного интеллекта. Сильный и слабый ИИ.
2. Логический, функциональный, агентный подход к ИИ. Интеллектуальные агенты.
3. Базы знаний. Экспертные системы. Инженерия знаний.
4. Самообучающиеся системы. Логический подход к обучению.
5. Принятие решений в условиях противодействия. Игровой интеллект.
6. Компьютерное зрение.
7. Задачи распознавания звука и понимания устной речи.
8. Роевой и муравьиный интеллект.
9. Биологический нейрон. Нейромедиаторы. Поляризация и деполаризация. Потенциалы действия (спайки).
10. Простейший формальный нейрон Мак-Каллока-Питтса.
11. Определение нейросети (НС). Типы архитектуры НС.
12. Перцептрон Розенблатта.
13. Перцептрон Румельхарта. Теорема об обучении перцептрона. Ограничение по линейной отделимости.
14. Сети прямого распространения (feed-forward). Теорема Колмогорова о полноте.

15. Алгоритм обратного распространения (backpropagation).
16. Алгоритмы первого порядка: delta-bar-delta, extended delta-bar-delta (EDBD).
17. Метод Ньютона для обучения НС.
18. Квазиньютоновские методы второго порядка: Левенберга-Марквардта, Поляка-Рибьера, BFGS и др.
19. Методы поиска глобального минимума функционала ошибки. Случайные старты. Метод отжига.
20. Генетические алгоритмы в обучении НС.
21. Самоорганизующаяся карта Кохонена.
22. Нейронная ассоциативная память (АП). Сети Хопфилда.
23. Двухнаправленная АП. Псевдоинверсная АП.
24. Ядерные методы в машинном обучении. Метод опорных векторов. Ядерная ассоциативная память.
25. Рекуррентные нейронные сети. Алгоритм backpropagation through time (BPTT).

Раздел «Кибербезопасность»

1. Принципы многоуровневой и эшелонированной защиты информации в компьютерных сетях.
2. Комплексное применение криптографических алгоритмов и систем в компьютерных сетях.
3. Криптопровайдеры. Принципы построения и использования криптоинтерфейса CryptoAPI.
4. Задачи и процедуры управления открытыми ключами.
5. Нормативно-правовая регламентация управления открытыми ключами. Необходимость защиты открытых ключей. Общие положения о сертификации и сертификатах.
6. Общие положения по применению цифровых сертификатов открытых ключей. Общие сведения о структуре цифрового сертификата открытого ключа.
7. Признаки и основные этапы реализации компьютерных атак.
8. Системы обнаружения и предупреждения компьютерных атак и их классификация. Требования, предъявляемые к системам обнаружения и предупреждения компьютерных атак.
9. Системы анализа защищенности: классификация, архитектура. Требования, предъявляемые к системам анализа защищенности.
10. Методика анализа защищенности автоматизированной системы.
11. Назначение и функции межсетевых экранов. Классификация межсетевых экранов и их характеристика.
12. Обобщенная структурная схема межсетевого экрана. Основные схемы подключения межсетевых экранов.
13. Организация безопасного межсетевого взаимодействия и удаленного доступа.
14. Защита информационного взаимодействия на канальном уровне.
15. Назначение и структура семейства протоколов IPSec.
16. Формат протоколов IKE, AH и ESP.
17. Система защиты информационных служб компьютерной сети.
18. Подходы, применяемые к обеспечению информационной безопасности в клиент-серверных информационно-вычислительных системах.
19. Виды аутентификации и разграничения доступа к информационным службам.
20. Архитектура протоколов защиты данных SSL и TLS. Процедура согласования параметров сеанса.
21. Особенности криптографических вычислений в протоколах SSL и TLS.
22. Протокол криптографической аутентификации и авторизации Kerberos.
23. Назначение, состав и возможности системы защиты электронной почты.

24. Функциональные возможности программного средства защиты электронной почты S/MIME.
25. Угрозы безопасности информации в базах данных. Система защиты информации в СУБД. Механизмы разграничения доступа в СУБД.

Литература

Математическое моделирование, численные методы и комплексы программ

1. Федоренко Р.П. Введение в вычислительную физику. – М.: Наука, 1994.
2. Каханер Д., Моулер К., Нэш С.. Численные методы и программное обеспечение. — М.: Мир, 1998.
3. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы. 5-е изд. – М.: БИНОМ. Лаборатория знаний, 2007 – 636 с.
4. Голуб Дж., Ван Лоун Ч. Матричные вычисления. Мир, 1999. – 548 с.
5. Деммель Дж. Вычислительная линейная алгебра. Теория и приложения. Мир, 2001. – 435 с.
6. Магарил-Ильяев Г.Г., Тихомиров В.М. Выпуклый анализ и его приложения. Изд-е 3-е. М.: УРСС, 2011.
7. Ибрагимов И.А., Хасьминский Р.З. Асимптотическая теория оценивания. М.: Наука, 1979.
8. V. Spokoiny. Basics of Modern Parametric Statistics. Springer, 2013 (см. <http://premolab.ru/sites/default/files/stat.pdf>).
9. Арутюнов А.В., Магарил-Ильяев Г.Г., Тихомиров В.М. Принцип максимума Понтрягина. Доказательство и приложения. М.: Факториал Пресс, 2006.
10. Айвазян С.А., Бухштабер В.М., Енюков С.А., Мешалкин Л.Д. Прикладная статистика. Классификация и снижение размерности. М.: Финансы и статистика, 1989.
11. Вьюгин В.В. Элементы математической теории машинного обучения. М.: Московский физико-технический институт (государственный университет) – ИППИ РАН, 2010. – 232
12. Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К. Алгоритмы: построение и анализ. – 2-е изд. – М.: Издательский дом «Вильямс», 2006.
13. Ахо А., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы. – М.: Издательский дом «Вильямс», 2000.
14. Вирт Н. Алгоритмы и структуры данных. – СПб.: Невский Диалект, 2005.
15. Керниган Б., Ритчи Д. «Язык программирования Си», 2-е издание, пер. с англ., М.: Финансы и статистика, 1992.
16. Страуструп Б. Язык программирования C++, 3-е издание, пер. с англ. - СПб.: Невский диалект, 1999 г.
17. Карпов В.Е., Коньков К.А. Основы операционных систем. Курс лекций. Учебное пособие. – М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий, 2005.
18. Гарсиа-Молина Г., Ульман Дж., Уидом Д. Системы баз данных. Полный курс. М.: Вильямс, 2004.
19. Якобсон А., Буч Г., Рамбо Дж. Унифицированный процесс разработки программного обеспечения. СПб.: Питер, 2002.

Теоретическая информатика, кибернетика

1. Габидулин Э. М., Пилипчук Н. И. Лекции по теории информации: Учебное пособие. – М.: МФТИ, 2007.
2. Попов, И. Ю. Теория информации : учебник / И. Ю. Попов, И. В. Блинова. — Санкт-Петербург : Лань, 2020. — 160 с. — ISBN 978-5-8114-4204-1.
3. Сагалович Ю.Л. Введение в алгебраические коды: Учебное пособие. – М.: МФТИ, 2007.
4. Габидулин Э.М., Кшевецкий А.С., Колыбельников А.И. Защита информации: Учебное пособие. – М.: МФТИ, 2017. – 262 с.

Искусственный интеллект и машинное обучение

1. С. Расселл, П. Норвиг. Искусственный интеллект. Современный подход. Вильямс, 2006г.
2. Bishop, Christopher M. Pattern recognition and machine learning. Vol. 4. No. 4. New York: springer, 2006.
3. С. Осовский. Нейронные сети для обработки информации. М., «Финансы и Статистика», 2004
4. Хайкин, Саймон. Нейронные сети: полный курс, 2-е издание. Издательский дом Вильямс, 2008.
5. Дж.Ф. Люгер. Искусственный интеллект. Стратегии и методы решения сложных проблем. Вильямс, 2003 г.
6. Саттон Р.С., Барто Э.Г. Обучение с подкреплением. — БИНОМ, 2011

Кибербезопасность

1. Стародубцев, Ю. И. Комплексная защита информации в локальных вычислительных сетях / Ю. И. Стародубцев, В. Е. Дементьев, М. А. Коцыняк. – Санкт-Петербург : ВАС, 2010. – 436 с.
2. Шангин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шангин. – Москва : ИД "Форум", 2010. – 592 с.
3. Запечников, С. В. Информационная безопасность открытых систем : учебник для вузов. В 2-х т. Т. 2. – Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская и др. – Москва : Горячая линия – Телеком, 2008. – 558 с.
4. Свечников, Д. А. Межсетевые экраны. В 2 ч. Ч. 1. / Д. А. Свечников и др. – Орёл : Академия ФСО России, 2013. – 170 с.
5. Комашинский, В. В. Методика применения криптопровайдеров для защиты прикладного программного обеспечения : учебно-методическое пособие / В. В. Комашинский. – Орёл : Академия ФСО России, 2010. – 182 с.
6. Свечников, Д. А., Комашинский, В. В. Яшин, А. А. Методические рекомендации по разработке программ для криптографической защиты информации / Д. А. Свечников, В. В. Комашинский, А. А. Яшин. – Орёл : Академия ФСО России, 2011. – 110 с.
7. Комашинский, В. В. Инфраструктура управления открытыми ключами : пособие / В. В. Комашинский. – Орёл : Академия ФСО России, 2010. – 230 с. : ил.
8. Основы информационной безопасности : учебное пособие / А. И. Козачок, А. А. Юркин, Н. И. Биркун и др. ; под ред. В. И. Козачка. – Орёл : Академия ФСО России, 2009. – 302 с.
9. Беляев, Д. Л. Компьютерная безопасность : практикум. В 2 ч. Ч. 1 / Д. Л. Беляев, В. В. Комашинский. – Орёл : Академия ФСО России, 2008. – 144 с.
10. Галицкий, А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – Москва : ДМК Пресс, 2004. – 616 с. : ил.
11. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учебное пособие для вузов / В. В. Платонов. – Москва : Академия, 2006. – 240 с. : ил.
12. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах / П. Б. Хорев. – Москва : Академия, 2008. – 256 с.
13. Защита от несанкционированного доступа к информации и требования по защите информации. Автоматизированные системы. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России. Руководящий документ. – Москва : Военное издательство, 1992. – 27 с.
14. Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Ч. 1. Гостехкомиссия России. – Москва : Военное издательство, 1999. – 6 с.

15. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России. Руководящий документ. – Москва : Военное издательство, 1992. – 9 с.
16. Шугуров, Д. Е. Методы и протоколы аутентификации / Д. Е. Шугуров и др. – Орёл : Академия ФСО России, 2013. – 219 с.
17. Международный стандарт ISO/IEC IS 27001:2005. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – Москва : ООО "GlobalTrust Solutions", 2005.
18. ГОСТ Р ИСО / МЭК 15408–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. Ч. 2. Функциональные требования безопасности. Ч. 3. Требования доверия к безопасности.
19. Комашинский, В. В. Управление доступом в компьютерных системах / В. В. Комашинский и др. – Орёл : Академия ФСО России, 2013. – 115 с.
20. Афанасьев, А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др. ; под ред. А. А. Ше-лупанова, С. Г. Груздева, Ю. С. Нахаева. – Москва : Горячая линия – Телеком, 2009. – 552 с. : ил.
21. Чипига, А. Ф. Информационная безопасность автоматизированных систем : учебное пособие для студентов вузов, обучающихся в обл. информ. безопасности / А. Ф. Чипига. – Москва : Гелиос АРВ, 2010. – 336 с. : ил.
22. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие для студ. учреждений высш. проф. образования / А. В. Черемушкин. – Москва : Издательский центр "Академия", 2009. – 272 с.
23. Гостехкомиссия России. Руководящий документ "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации". – Москва : Военное издательство, 1997.
24. Поляков, А. М. Безопасность Oracle глазами аудитора: нападение и защита. – Москва : ДМК Пресс, 2010. – 336 с. : ил.