МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Казанский (Приволжский) федеральный университет»
Институт физики

УТВЕРЖДАЮ
Проректор по
образовательной деятельности
_____ Е.А. Турилова
«___» _____ 2024 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Направление подготовки: 10.04.01 Информационная безопасность

Магистерские программы: Информационная безопасность автоматизированных систем

Форма обучения: очная

2024

Лист согласования программы вступительного испытания

Разработчик(и) программы: Шерстюков О. Н. – заведующий кафедрой радиофизики;

Корчагин П. А. – старший преподаватель кафедры радиофизики

Председатель экзаменационной комиссии 
О. Н. Шерстюков

Программа вступительного испытания обсуждена и одобрена на заседании кафедры радиофизики Института физики, Протокол № 8 от «19» сентября 2024 г.

Решением Учебно-методической комиссии Института физики Программа вступительного испытания рекомендована к утверждению Ученым советом, Протокол № 2 от «7» октября 2024 г.

Программа вступительного испытания утверждена на заседании Ученого совета Института физики, Протокол № 2 от «17» октября 2024 г.

Раздел 1. Вводная часть

1.1 Цель и задачи вступительных испытаний

Вступительные испытания предназначены для определения теоретической и практической подготовленности абитуриентов и проводятся с целью определения соответствия знаний, умений и навыков требованиям обучения в магистратуре по направлению 10.04.01 - Информационная безопасность, наименование программ «Информационная безопасность автоматизированных систем». Программа вступительного испытания предназначена для подготовки абитуриента к вступительному экзамену по вышеуказанному направлению магистратуры, реализуемому в Институте физики Казанского федерального университета.

Цель вступительного испытания выявить способности и готовность абитуриента к обучению по основной образовательной программе подготовки магистров. В ходе испытания оцениваются обобщенные знания и умения по дисциплинам направления; выявляется степень сформированности компетенций, значимых для успешного освоения магистерской программы.

1.2 Общие требования к организации вступительных испытаний

К вступительным испытаниям допускаются граждане Российской Федерации и граждане иностранных государств, успешно завершившие обучение по одной из основных образовательных программ высшего образования и имеющие документ государственного образца: диплом бакалавра, диплом магистра, диплом специалиста.

Руководство по организации и проведению вступительных испытаний осуществляют председатели экзаменационных комиссий, которые несут всю полноту ответственности за соблюдение законодательства Российской Федерации, требования ФГОС ВО, локальных документов о подготовке и проведении вступительных испытаний.

Проведение вступительных испытаний осуществляется в соответствии с принципами: соблюдения прав и свобод граждан, установленных законодательством Российской Федерации, гласности и открытости результатов вступительных испытаний, объективности оценки способностей абитуриентов и единообразия оценки вступительных испытаний.

Прием в магистратуру осуществляется на конкурсной основе по результатам вступительных испытаний.

Для поступающих проводятся консультации по содержанию программы вступительных испытаний и критериям оценки знаний, умений, компетенций абитуриентов.

На вступительных испытаниях должна быть обеспечена спокойная и доброжелательная обстановка, предоставлена возможность поступающим наиболее полно проявить уровень сформированности знаний, умений, компетенций.

Во время вступительных испытаний поступающему запрещается пользоваться учебниками, справочными материалами, тетрадями, записями, мобильными телефонами, электронными записными книжками и другими средствами хранения информации.

Присутствие на вступительных испытаниях посторонних лиц не допускается.

Результаты вступительных испытаний оцениваются по 100-бальной шкале. Решение экзаменационной комиссии заносится в протокол.

1.3 Описание формы проведения вступительных испытаний

Вступительные испытания проводятся в форме профессионально-ориентированного собеседования очно и (или) с использованием дистанционных технологий.

Инструкция по проведению экзамена в дистанционной форме на платформе MicrosoftTeams

1. Необходимо скачать программу MicrosoftTeams (https://teams.microsoft.com/downloads) для настольного компьютера или устройства с iOS/Android. Также можно работать на платформе MicrosoftTeams, загружая ее в браузере с сайта https://teams.microsoft.com.

2. Перед проведением консультации и экзамена на e-mail абитуриента, который был им указан при регистрации в электронной форме через социально-образовательную сеть КФУ «Буду студентом!», будет отправлено письмо-приглашение в Команду, в которой будет проходить экзамен.
3. Необходимо пройти по ссылке, указанной в письме, и зарегистрироваться в MicrosoftTeams, используя электронный адрес, на который пришло приглашение.
4. После регистрации на платформе MicrosoftTeams абитуриенту будет доступна команда, в которой будет проходить экзамен.
5. В назначенное по расписанию время проведения консультации и экзамена необходимо зайти в команду и присоединиться к собранию.
6. Экзамен будет проходить только в режиме видеоконференцсвязи в режиме реального времени строго по расписанию.
7. Для идентификации личности на экзамене абитуриенту необходимо предоставить паспорт.
8. На подготовку ответа на полученный билет отводится не более 40 минут
9. Устный ответ заслушивается только при полном видео и аудио контакте преподавателя и отвечающего.
10. Продолжительность ответа каждого абитуриента, в том числе на дополнительные вопросы – не более 20 минут.

1.4 Продолжительность вступительных испытаний в часах

Общая продолжительность вступительных испытаний – до 60 мин, включая время для подготовки – до 40 мин., собеседование – до 20 мин на каждого абитуриента.

1.5 Структура вступительных испытаний

Собеседование включает в себя:

Профильный модуль: собеседование по предметному блоку.

Раздел 2. Содержание программы

Вступительные испытания по направлению магистратуры (10.04.01 - Информационная безопасность) охватывают стандартные разделы университетского курсов: дискретная математика, основы информационной безопасности, языки программирования, безопасность базы данных, технические средства защиты информации. Также проверяются базовые умения математического аппарата. Вопросы и структура экзаменационных билетов приведены в разделе 3.

Экзаменующийся должен показать степень **знания** основных понятий, законов и моделей радиофизики; он должен иметь представление о ее современном состоянии. Он должен **уметь** понимать, излагать и критически анализировать базовую общефизическую информацию; пользоваться теоретическими основами, основными понятиями, законами и моделями; формулировать и доказывать основные результаты физики. Он должен **владеть** базовым математическим аппаратом и основными навыками решения задач по курсам теоретической и общей физики в приложении к волновым явлениям. Обучающийся должен **демонстрировать** способность и готовность к дальнейшему обучению.

Раздел 3. Фонд оценочных средств

3.1 Примерный перечень вопросов для собеседования по профильному модулю

Программа испытания

Дискретная математика

1. Функции алгебры логики. Реализация функций формулами. Канонические
2. формы представления функций (ДНФ, КНФ, СДНФ, СКНФ, полином Жегалкина).
3. Замыкание систем функций алгебры логики. Основные замкнутые классы.

4. Полнота систем функций алгебры логики. Критерий функциональной полноты.
5. Проблема построения минимальных дизъюнктивных нормальных форм и подходы к ее решению.
6. Детерминированные и ограниченно детерминированные функции. Способы
7. задания ограниченно-детерминированных функций.
8. Проблематика теории кодирования. Алфавитное кодирование. Проблема однозначности кодирования. Префиксные коды.
9. Коды с минимальной избыточностью (Коды Хафмана).
10. Помехоустойчивое кодирование. Коды Хемминга.
11. Языки, грамматики и их классификация. Примеры контекстно-свободных
12. грамматик.
13. Графы. Способы задания графов. Геометрическая реализация графов.
14. Обходы графа в глубину и в ширину. Вычисление числа компонент связности графа.
15. Алгоритмы поиска путей в графе.
16. Алгоритмы нахождения минимального остова графа.
17. Транспортные сети. Теорема Форда-Фалкерсона о максимальном потоке в транспортной сети.

Основы программирования

1. Рекурсивные программы и их особенности.
2. Особенности объектно-ориентированного программирования.
3. Механизмы управления памятью.
4. Базовые типы в языках программирования.
5. Механизмы создания новых типов данных.
6. Алгоритмы и языки их описания.
7. Основные средства и особенности процедурных языков программирования.
8. Процедуры и функции. Описание и использование.
9. Абстрактные типы данных – стеки, очереди.
10. Макросредства и препроцессоры.
11. Алгоритмы сортировки. Оценка вычислительной сложности алгоритмов сортировки.
12. Алгоритмы поиска. Оценка вычислительной сложности алгоритмов поиска.
13. Линейные списки и алгоритмы их обработки.
14. Деревья и алгоритмы их обработки.
15. Символьные строки и их обработка.
16. Трансляция арифметических выражений.

17. Классы. Свойства и методы, защита элементов классов. Создание и уничтожение объектов.

18. Наследование в классах.

Базы данных

1. Ключи, индексы, внешние ключи.
2. Запросы к базам данных, их типы. Типы связей между таблицами.
3. Основные операторы языка SQL по созданию таблиц, изменению данных, выполнению выборки.
4. Связи между таблицами в базах данных. Ссылочная целостность (схема данных).
5. Проектирование баз данных. Метод ER-диаграмм.
6. Архитектура информационных систем. Модели «клиент-сервер».
7. Методы доступа к базам данных с использованием технологии ASP.
8. Доступ к базам данных с помощью PHP.
9. Системное и прикладное программное обеспечение
10. Назначение и основные функции операционных систем.
11. Назначение и основные функции файловых систем.
12. Программные средства для работы в глобальной компьютерной сети INTERNET.
13. Организация взаимодействия процессов в компьютерных сетях. Стек протоколов TCP/IP.
14. Процессы жизненного цикла разработки программного обеспечения.

Основы информационной безопасности

1. Понятие национальной безопасности.
2. Виды безопасности: экономическая внутриполитическая, социальная, военная. международная, информационная, экологическая и другие.
3. Соотношение безопасности личности, общества и государства.
4. Виды защищаемой информации.
5. Правовые, организационно-технические и экономические методы обеспечения ИБ.
6. Модели, стратегии и системы обеспечения ИБ.
7. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
8. Методы и средства обеспечения ИБ компьютерных систем.
9. Информационная безопасность и информационное противоборство.
10. Методы нарушения конфиденциальности, целостности и доступности информации.
11. Причины, виды, каналы утечки и искажения информации.

12. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны

Методы инженерно-технической защиты информации

1. Классификация методов инженерно-технической защиты информации.
2. Инженерная защита и техническая охрана объектов.
3. Методы инженерной защиты и технической охраны объектов.
4. Методы скрытия информации и ее носителей.
5. Пространственное скрытие объектов наблюдения и сигналов.
6. Структурное и энергетическое скрытие объектов наблюдения.
7. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение.
8. Энергетическое скрытие радио и электрических сигналов.
9. Виды и условия зашумления сигналов.
10. Акустоэлектрические преобразования.
11. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.
12. Физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям

Раздел 4. Список литературы

1. Масленников М. Практическая криптография. С.-П.: БХВ – Петербург, 2003.

2. Ерош И.Л., Сергеев М.Б., Соловьев Н.В. Дискретная математика: Учебное пособие для вузов. - СПб.: ГУАП, 2005. - 142 с.

3. Лунгу К. Н. Линейное программирование. Руководство к решению задач. - М.: ФИЗМАТЛИТ, 2005. - 128 с.

4. В. В. Кириллов, Г. Ю. Громов. Введение в реляционные базы данных. Издательство: БХВ-Петербург Год: 2009

5. Х.М. Дейтл «Операционные системы: Основы и принципы» -Москва «Бином» 2009.

6. С. Орлов. Теория и практика языков программирования. Учебник для вузов. Стандарт 3-го поколения. — СПб.: Питер, 2013. — 688 с.

7.Основы информационной безопасности, Расторгуев, Сергей Павлович, 2007г.

8. Информационная безопасность, Бабаш, Александр Владимирович; Баранова, Елена Константиновна; Мельников, Юрий Николаевич, 2012г.

9. Информационная безопасность, Партыка, Татьяна Леонидовна;Попов, Игорь Иванович, 2007г.

10.Торокин А. А. Основы инженерно-технической защиты информации. М: "Ось-89", 365 с.

11. Хорев А. А. Способы и средства защиты информации. М.: МО РФ, 1998, 316 с.

12. Петраков А. В., Дорошенко П. С., Савлуков Н. В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 1999, 568 с.

13. Организация и современные методы защиты информации. /Под общей редакцией С. А.

14. Диева и А. Г. Шаваева. М.: Концерн "Банковский Деловой Центр", 1998, 472 с.

15. Петраков А. В. Основы практической защиты информации. М.: Радио и связь, 1999, 368 с.