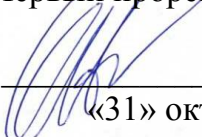


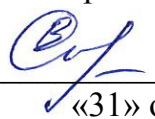
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

**Национальный исследовательский ядерный университет «МИФИ»
(НИЯУ МИФИ)**

УТВЕРЖДАЮ
Первый проректор НИЯУ МИФИ


О.В. Нагорнов
«31» октября 2023 г.

Ответственный секретарь
приемной комиссии


В.И. Скрытный
«31» октября 2023 г.

**Программа вступительного испытания
по направлению подготовки магистров
10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
Образовательная программа
«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ»**

Форма обучения
Очно-заочная (вечерняя)

Москва 2023

ОБЩИЕ ПОЛОЖЕНИЯ

Программа вступительного испытания сформирована на основе федеральных государственных образовательных стандартов высшего образования.

Форма проведения испытания:

Вступительное испытание в магистратуру проводится в форме собеседования с обязательным оформлением ответов на вопросы билета в письменном виде. Собеседование проводится с целью выявления у абитуриента объема знаний, необходимых для обучения в магистратуре.

Структура испытания:

Испытание состоит из ответов на вопросы билета и дополнительные вопросы в рамках программы вступительного испытания. Билет состоит из 2 вопросов. Один вопрос выбирается из перечня общих вопросов программы вступительного испытания, второй вопрос выбирается из перечня вопросов профильной части образовательной программы.

Оценка испытания:

Оценка за собеседование выставляется по 100-балльной шкале. Минимальный балл, необходимый для успешного прохождения собеседования и дальнейшего участия в конкурсе ежегодно устанавливается приемной комиссией НИЯУ МИФИ.

Критерии оценки результатов испытания:

100-95 баллов - даны исчерпывающие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует глубокие теоретические знания, умение сравнивать и оценивать различные научные подходы, пользоваться современной научной терминологией.

94-90 баллов - даны полные, достаточно глубокие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания, умение пользоваться современной научной терминологией.

89-75 баллов - даны обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания.

74-60 баллов - даны в целом правильные ответы на вопросы, поставленные экзаменационной комиссией, при этом абитуриент недостаточно аргументирует ответы.

59-0 баллов – абитуриент демонстрирует непонимание основного содержания теоретического материала, поверхностность и слабую аргументацию суждений или допущены значительные ошибки.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

Перечень общих вопросов

1. Теория информационной безопасности

Место проблем защиты информации в общей совокупности информационных проблем современного общества. Определение информационной безопасности, защиты информации и системы защиты информации. Основные требования, предъявляемые к системе защиты информации. Риски информационной безопасности. Уязвимости информационных систем. Системная классификация угроз безопасности информации.

2. Физика. Электричество и магнетизм.

Потенциал. Эквипотенциальные поверхности. Связь между напряженностью электрического поля и его потенциалом. Проводник во внешнем электрическом поле. Диполь, его поведение в электрическом поле. Энергия электрического поля, плотность энергии. Электродвижущая сила источника тока. Закон Ома для однородного и для неоднородного участков цепи. Сопротивление и проводимость проводников. Сила взаимодействия параллельных токов. Контур с током в однородном магнитном поле: сила и вращательный момент, действующие на контур. Напряженность магнитного поля. Относительная магнитная проницаемость вещества. Энергия магнитного поля тока. Плотность энергии. Вычисление полей заданных токов с помощью теоремы о циркуляции магнитного поля.

3. Теория вероятностей и математическая статистика

Случайные величины, функции распределения, их свойства. Типовые распределения: биномиальное, пуассоновское, нормальное. Схема Бернулли и полиномиальная схема. Независимость событий. Условные вероятности, формулы Байеса. Математическое ожидание и дисперсия случайной величины. Цепи Маркова, их свойства. Задача проверки статистических гипотез. Статистические критерии. Ошибки 1-го и 2-го родов при проверке гипотез. Метод статистических испытаний. Оценка результатов измерений. Точечные оценки и их определение. Надёжность оценки, доверительная вероятность и доверительный интервал.

4. Организационное и правовое обеспечение информационной безопасности

Основные положения доктрины информационной безопасности Российской Федерации основные положения доктрины информационной безопасности от 5 декабря 2016 г. Основные положения стратегии национальной безопасности Российской Федерации от 31 декабря 2015 г. Государственная система защиты информации и ее структура. Лицензирование, сертификация и аттестация в области защиты информации. Основные положения Федеральных Законов РФ: № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», № 152-ФЗ от 27.07.2006 «О персональных данных», № 5485-1 от 21.07.1993 «О государственной тайне», № 98-ФЗ от

29.07.2004 «О коммерческой тайне», № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации». Преступления в области защиты информации (Уголовный кодекс РФ, Гражданский кодекс РФ, Кодекс об административных правонарушениях РФ).

Перечень профильных вопросов

1. Технические каналы утечки информации

Модель технического канала утечки информации. Технические каналы утечки акустической и речевой информации. Основные характеристики. Технические каналы утечки информации при передаче по каналам связи. Основные характеристики. Технические каналы утечки информации средств вычислительной техники. Основные характеристики. Технические каналы утечки видовой информации. Основные характеристики.

2. Защита информации от несанкционированного доступа

Методы идентификации и аутентификации, общая характеристика функции аутентификации. Методы реализации контроля и разграничения доступа. Функции контроля и разграничения доступа. Модель нарушителя доступа при защите автоматизированных систем от несанкционированного доступа. Методы контроля защищенности автоматизированных систем от несанкционированного доступа. Аппаратно-программные средства защиты информации от несанкционированного доступа.

3. Защита от вредоносного программного обеспечения.

Общее описание компьютерных вирусов. Видовая классификация компьютерных вирусов. Методы и средства антивирусной защиты. Организационно-правовые меры. Защита от вирусов в статике процессов. Защита от вирусов в динамике процессов. Антивирусная политика на объекте информатизации. Основные направления антивирусной борьбы в компьютерных и телекоммуникационных системах. Основные механизмы внедрения компьютерных вирусов в поражаемую систему.