МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
(НИЯУ МИФИ)

УТВЕРЖДАЮ
Проректор НИЯУ МИФИ
_____В.В. Ужва

СОГЛАСОВАНО
Ответственный секретарь
приемной комиссии
_____В.И. Скрытный

Программа вступительного испытания
по направлению подготовки магистров
10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Форма обучения
Очная

Москва 2016

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 объёма 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 3 вопросов. Два вопроса выбираются из перечня общих вопросов программы вступительного испытания, третий вопрос выбирается из перечня вопросов профильной части согласно выбранному абитуриентом профилю 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.

89-85 баллов - даны обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания.

84-80 баллов - даны в целом правильные ответы на вопросы, поставленные экзаменационной комиссией, при этом абитуриент недостаточно аргументирует ответы.

79-0 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. Постановка задачи защиты информации. Современные задачи защиты информации. Риски информационной безопасности. Уязвимости информационных систем. Системная классификация угроз безопасности информации.

2. Теория информации

Понятие информации. Жизненный цикл информации. Количество информации и энтропия. Формулы Хартли и Шеннона. Математические модели каналов связи. Помехоустойчивость каналов. Типы сигналов, их дискретизация и восстановление. Сжимающее и помехоустойчивое кодирование. Способы адресации в сетях. Управление потоками. Маршрутизация пакетов. Защита от перегрузок.

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-ого и 2-ого родов при проверке гипотез. Метод статистических испытаний. Оценка результатов измерений. Точечные оценки и их определение. Надёжность оценки, доверительная вероятность и доверительный интервал.

4. Технологии программирования, алгоритмы и структуры данных

Жизненный цикл программного обеспечения. Тестирование программ. Принципы разработки параллельных методов программирования. Основные алгоритмы поиска данных, их временная сложность. Алгоритмы сортировки, их временная сложность и практическое значение для решения задач обработки данных.

5. Организационное и правовое обеспечение информационной безопасности

Основные положения Доктрины информационной безопасности Российской Федерации. Стратегия национальной безопасности Российской Федерации. Государственная система защиты информации и ее структура. Лицензирование, сертификация и аттестация в области защиты информации. Основные положения закона РФ «Об информации, информационных технологиях и о защите информации», закона РФ «О персональных данных». Основные положения Федеральных Законов РФ «О государственной тайне», «О коммерческой тайне». Преступления в области защиты информации (Уголовный кодекс РФ, Гражданский кодекс РФ, Кодекс об административных правонарушениях РФ).

6. 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.

Перечень вопросов профильной части

Профиль «ПРИМЕНЕНИЕ МЕТОДОВ КРИПТОЛОГИИ В СИСТЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1. Алгебра

Определение группоида, полугруппы, моноида, группы, кольца, поля. Циклические группы и их свойства. Полугруппа преобразований, группа подстановок. Теорема Кэли. Кольцо многочленов над полем, НОД и НОК многочленов, алгоритм Евклида. Кольцо вычетов по модулю натурального числа. Кольцо матриц. Линейное пространство над полем, базис и размерность линейного пространства. Решение систем линейных уравнений.

2. Булевы функции и автоматы

Булевы функции, их характеристики. Способы задания булевых функций. Полнота системы булевых функций. Конечные автоматы Мили. Виды автоматов. Отношения и операции над автоматами. Эквивалентность состояний и автоматов. Теорема Хаффмана-Мили

3. Основы криптографической защиты информации

Обеспечение секретности, подлинности (аутентичности), целостности, неотказуемости от авторства, неотслеживаемости (анонимности) с помощью криптографических методов. Определение криптографической системы, виды криптосистем. Базовые криптографические примитивы. Шифры перестановки и замены. Блочные и поточные шифры. Понятие о криптографическом протоколе. Трехэтапный протокол Шамира.

Профиль «Обеспечение безопасности информации ключевых систем информационной инфраструктуры»

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.

Профиль «Обеспечение непрерывности и информационной безопасности бизнеса»

1. Комплексные системы зашиты информации (КСЗИ)

Системный подход при комплексной защите информации. Объект защиты. Системность и комплексность защиты информации. Макроструктурные компоненты комплексной системы зашиты информации (функциональные и обеспечивающие подсистемы). Подсистемы обеспечения информационной безопасности. Процессный подход к обеспечению информационной безопасности. Политики обеспечения информационной безопасности. Управление информационной безопасностью. Информационная безопасность в аспекте управления персоналом. Организационно-правовые меры защиты информации.

2. Сетевая безопасность

Понятия интранета, экстранета и портала. Угрозы ИБ их ресурсам. Специфика информационной безопасности в сетях. Политика обеспечения безопасности для сетей. Обеспечение конфиденциальности, целостности, доступности, аутентичности, неотказуемости, учетности и надежности в сетевой среде. Программно-аппаратные средства обеспечения ИБ в сетях. Уязвимости и угрозы информационной безопасности в сетевой среде. Примеры распространённых удаленных атак на сетевые ресурсы. Средства реализации атак. Аутентификация в сетях. Уязвимости, угрозы и средства защиты в интернете.

Профиль «Информационно-аналитическое обеспечение финансового мониторинга»

1. Международные стандарты противодействия легализации преступных доходов и финансированию терроризма

История возникновения понятия отмывание денег. Юридическое определение отмывания денег. Общественная опасность отмывания денег. Понятие финансирование терроризма. Сущность и источники финансирования терроризма. Связь финансирования терроризма с отмыванием денег. Институциональные основы международной системы ПОД/ФТ. Характеристики международной системы ПОД/ФТ. Типовая система ПОД/ФТ: структура, элементы. Международные стандарты в сфере ПОД/ФТ: криминализация отмывания денег и финансирования терроризма, ответственность юридических лиц. Регулирование и надзор в целях ПОД/ФТ. Создание ПФР, его функции и типы. Полномочия и ресурсы правоохранительных органов сферы ПОД/ФТ. Условия и принципы международного сотрудничества в сфере ПОД/ФТ. Принципы обмена информацией между ПФР. Сотрудничество между правоохранительными и надзорными органами в сфере ПОД/ФТ. Документы Базельского комитета по банковскому надзору по линии ПОД/ФТ. Последовательность взаимной оценки элементов системы ПОД/ФТ, условия и задачи проведения миссий взаимной оценки в сфере ПОД/ФТ. Отраслевые рынки и виды экономической деятельности в типологических исследованиях ФАТФ. Участие России в международной системе ПОД/ФТ.

2. Базы данных

Основные понятия: определение данных, системы баз данных. Основные этапы проектирования баз данных. История развития СУБД. Представление статических и динамических свойств реального мира. Базовые структурные компоненты модели данных: домены и атрибуты, отношение сущности, схема отношения. Общая характеристика ограничений целостности. Уровни абстракции представления данных. Информация о сущностях и связях. Типы ограничений целостности. Реляционная модель данных. Средства языка SQL как языка описания данных. Описание структуры и ограничений целостности (предложение CREATE TABLE). Формирование запросов. Предложение SELECT. Проектирование реляционных баз данных: возникающие проблемы, основные цели проектирования. Функциональные зависимости. Определение ключа. Назначение и

суть индексирования. Структуры типа двоичное дерево, многоходовое дерево. Методы доступа к данным в БД. Структуры типа B-дерево.