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

УТВЕРЖДАЮ:
Ответственный секретарь
приемной комиссии
_____В.И. Скрытный
«15» января 2026 г.

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

Форма обучения
Очная

Москва 2026

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 2 вопросов. Один вопрос выбирается из перечня общих вопросов программы вступительного испытания, второй 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 и системы защиты информации. Основные требования, предъявляемые к системе 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.

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. Технологии программирования, алгоритмы и структуры данных

Жизненный цикл программного обеспечения. Тестирование программ. Параллельные методы программирования. Основные алгоритмы поиска данных, их временная сложность. Алгоритмы сортировки, их временная сложность и практическое значение для решения задач обработки данных. Сравнительные оценки алгоритмов. Оценка времени выполнения программ. Основные абстрактные типы данных: списки, стеки, очереди, деревья, ориентированные и неориентированные графы.

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 Федеральных законов РФ «О безопасности», «Об информации, информационных технологиях и о защите информации», «О безопасности критической информационной инфраструктуры Российской Федерации». Основные положения Федеральных Законов РФ «О государственной тайне», «О коммерческой тайне», «О персональных данных». Преступления в области защиты информации (Уголовный кодекс РФ, Гражданский кодекс РФ, Кодекс об административных правонарушениях РФ).

Перечень вопросов по образовательным программам

образовательная программа «Безопасность данных и криптография»

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, целостности, неотказуемости от авторства с помощью криптографических методов. Определение криптографической системы, виды криптосистем. Базовые криптографические примитивы. Шифры перестановки и замены. Блочные и поточные шифры. Вычислительно сложные задачи и однонаправленные функции, используемые в криптографии. Электронная цифровая подпись. Криптографические хэш-функции. Понятие о криптографическом протоколе. Свойства протокола.

образовательная программа «Теоретическая и практическая криптография»

1. Дискретная математика

Отношения на множествах: рефлексивные, симметричные, антисимметричные, транзитивные, эквивалентные. Отображения множеств: сюръективные, инъективные, биективные. Принцип математической индукции. Определения сочетания, размещения, перестановки. Число сочетаний и его свойства, формула бинома Ньютона. Определения ориентированного и неориентированного графов. Способы задания и примеры графов. Определение булевой функции. Способы задания булевой функции: дизъюнктивные и конъюнктивные нормальные формы; многочлен Жегалкина.

2. Основы теории чисел

Функция Эйлера. Малая теорема Ферма. Алгоритм Евклида и теорема Ламе, расширенный алгоритм Евклида. Основная теорема арифметики. Вероятностные тесты на простоту. Сравнения первой степени. Китайская теорема об остатках. Квадратичные сравнения, символы Лежандра и Якоби.

3. Основы высшей алгебра

Множества с бинарными операциями; ассоциативность, коммутативность, дистрибутивность бинарных операций. Таблица Кели. Группа. Определение подстановки; группа подстановок. Определения кольца, поля. Кольцо вычетов $\mathbb{Z}_m$ по модулю натурального числа m.

4. Основы криптографии

Понятие криптографической системы (функции зашифрования, функция расшифрования, ключ, открытый текст, шифртекст). Шифры замены и перестановки. Симметричная криптография. Современные симметричные криптосистемы. Базовые методы криптографического анализа (полный перебор, частотный). Асимметричная криптография. Выработки общего секретного ключа по открытому каналу. Протокол Диффи-Хеллмана. Криптосистема RSA. Понятие электронной подписи. Криптографические методы обеспечения целостности информации. Бесключевые и ключевые функции хеширования. Криптографические протоколы TLS, IPsec, SSH.

Образовательные программы
«Обеспечение кибербезопасности и киберустойчивости объектов»
«Центры обнаружения и предотвращения компьютерных атак»

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. Способы адресации в сетях. Управление потоками. Маршрутизация пакетов.

Образовательная программа «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.

Перечень рекомендованной литературы

Основная литература:

1. К. Дж. Дейт Введение в системы баз данных. – Вильямс, 2018 г.
2. Г. Гарсиа-Молина, Дж. Ульман, Дж. Уидом Системы баз данных полный курс. – Вильямс, 2017 г.
3. Коннолли Т., Бегг К. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – Вильямс, 2017 г.
4. Алексеева Д.Г., Пыхтин С.В. Правовые основы обеспечения финансовой устойчивости кредитных организаций: учеб. пособие для бакалавриата и магистратуры. – М.: Издательство Юрайт, 2017. – 90 с.
5. Иванов А.В. Противодействие легализации преступных доходов в системе мер обеспечения экономической безопасности. М: Угрешская типография, 2018. – 212 с.
6. Годес Н.В. Финансовый контроль: курс лекций. – Минск: Право и экономика, 2018. – 468 с.
7. Русанов Г.А. Противодействие легализации (отмыванию) преступных доходов: учеб. пособие для бакалавриата и магистратуры. – М.: Издательство Юрайт, 2017. – 157 с.
8. Чернов С.Б. Противодействие финансированию терроризма. – М.: 2018. – 128 с.
9. Шашкова А.В. Правовое регулирование противодействия отмыванию доходов, полученных преступным путем. – М: Издательство Юрайт, 2017. – 272 с.
10. Соломатина Е.А. Противодействие легализации преступных доходов: методическое пособие. – М.: Издательство «Юнити-Дана», 2017. – 79 с

Дополнительная литература:

1. Пржиялковский В.В. Введение в Oracle SQL, Москва: ИНТУИТ, 2016
2. ЭИ А79 Системы управления базами данных (СУБД) : учебное пособие для иностранных студентов, Москва: НИЯУ МИФИ, 2014