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
_____ Скрытный В.И.
«15» января 2026 г.

Программа вступительного испытания по специальной дисциплине

Информационная безопасность

Научная специальность

2.3.6. «Методы и системы защиты информации, информационная безопасность»

Форма обучения
очная

Москва, 2026

Оглавление

1. Общие положения

Форма проведения испытания:

Целью вступительного испытания является выявления у абитуриента объёма научных знаний, научно-исследовательских компетенций, навыков системного и критического мышления, необходимых для подготовки диссертации по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность». Абитуриент должен показать профессиональное владение теорией и практикой в предметной области, продемонстрировать умение вести научную дискуссию, умение планировать научную работу в рамках выбранной научной специальности. Вступительное испытание проводится в форме экзамена с элементами собеседования.

Вступительное испытание состоит из двух частей.

В первой части абитуриент отвечает на вопросы из билета. Билет включает в себя два вопроса. Абитуриент после получения билета подготавливает ответ, фиксируя основные тезисы на бланке для ответов, после чего отвечает на вопросы билета перед экзаменаторами. Экзаменаторы могут задавать дополнительные вопросы согласно программе вступительных испытаний.

Выявление факта пользования мобильным телефоном или шпаргалками ведет к безусловному удалению абитуриента с вступительного испытания и составлению соответствующего протокола. Абитуриент из конкурса выбывает.

Во второй части абитуриент представляет заранее подготовленные тему планируемого диссертационного исследования в соответствии с выбранной научной специальностью, обоснование актуальности темы, а также план выполнения диссертационного исследования. Представленные материалы оценивается экзаменаторами. В процессе оценивания экзаменаторы могут уточнять различные аспекты, связанные с планируемым диссертационным исследованием.

Оценка испытания:

Оценка за вступительное испытание выставляется по 100-балльной шкале как сумма за первую и вторую часть испытания.

Максимальное число баллов за первую часть – 50 баллов.

Максимальное число баллов за вторую часть – 50 баллов.

Минимальный суммарный балл, необходимый для успешного прохождения испытания и дальнейшего участия в конкурсе – 60 баллов.

Критерии оценки результатов испытания

Вопрос № 1, 2	**0-25 баллов за каждый вопрос**	23-25 баллов – дан исчерпывающий и обоснованный ответ на вопрос, абитуриент демонстрирует глубокие теоретические знания, умение сравнивать и оценивать различные научные подходы, пользоваться современной научной терминологией. 19-22 баллов – дан полный, достаточно глубокий и обоснованный ответ на вопрос, поставленный экзаменационной комиссией, абитуриент демонстрирует хорошие знания, умение пользоваться современной научной терминологией. 15-18 баллов – даны обоснованные ответы на вопрос, поставленный экзаменационной комиссией, абитуриент демонстрирует хорошие знания. 11-14 баллов - даны в целом правильные ответы на вопрос, поставленный экзаменационной комиссией, при этом абитуриент недостаточно аргументирует ответы. 0-10 баллов – абитуриент демонстрирует непонимание основного содержания теоретического материала, поверхностность и слабую аргументацию суждений или допущены значительные ошибки.
Оценка планируемого диссерта-ционного исследования	**0-50 баллов**	45-50 баллов – предполагаемая тематика соответствует паспорту научной специальности, является актуальной, план работы над диссертации представлен на высоком уровне. 35-44 баллов – предполагаемая тематика соответствует паспорту научной специальности, является актуальной, план работы над диссертацией требует доработки. 25-34 баллов – предполагаемая тематика в целом соответствует паспорту научной специальности, но требует доработки в части актуальности, план работы над диссертацией требует доработки. 15-24 баллов - предполагаемая тематика в целом соответствует паспорту научной специальности, но требует значительной доработки в части актуальности, и значительной переработки плана работы над диссертацией. 0-14 баллов – предполагаемая тематика не соответствует паспорту научной специальности.

2. Вопросы для подготовки к первой части вступительного испытания

ОСНОВЫ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Информатика и системы передачи данных

1. Информация, данные, сигналы. Источники информации и ее носители. Жизненный цикл информации.
2. Количество информации и энтропия. Формула Шеннона.
3. Математические модели каналов связи. Помехоустойчивость каналов.
4. Типы сигналов, их дискретизация и восстановление.
5. Спектральная плотность сигналов. Теорема Котельникова.
6. Частотное представление дискретных сигналов. Ортогональные преобразования дискретных сигналов. Задачи интерполяции и прореживания сигналов.
7. Характеристики процесса передачи информации. Математические модели каналов связи и их классификация.
8. Аналого-цифровое и цифро-аналоговое преобразование. Быстрые преобразования. Цифровые фильтры.
9. Нелинейное и параметрическое преобразование сигналов. Модуляция и демодуляция; преобразование частоты.

Теория вероятностей и математическая статистика

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

Технологии программирования, алгоритмы и структуры данных

1. Жизненный цикл программного обеспечения. Тестирование программ.
2. Параллельные методы программирования.
3. Основные алгоритмы поиска данных, их временная сложность.
4. Алгоритмы сортировки, их временная сложность и практическое значение для решения задач обработки данных.

5. Временная сложность алгоритмов. Оценка времени выполнения программ.
6. Основные абстрактные типы данных: списки, стеки, очереди, деревья, ориентированные и неориентированные.

Вычислительные сети

1. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основы организации и функционирования сетей.
2. Распределенная обработка информации в системах клиент-сервер; одноранговые сети.
3. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения прав доступа.
4. Глобальная сеть Internet: основные службы и предоставляемые услуги, основные протоколы, особенности реализации на различных платформах, стандарты.
5. Глобальная сеть Internet: технологии обеспечения безопасности, функционирование, разработка и сопровождение приложений.
6. Современные виды информационного обслуживания; электронная почта; телеконференция; видеотекс; сети связи; структура, топология и архитектура сетей связи.
7. Методы коммутации информации; особенности сетей с коммутацией каналов, сообщений и пакетов.
8. Глобальные и локальные сети; особенности современных сетевых архитектур; архитектурные особенности современных локальных сетей; протоколы физического и канального уровней.

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основы криптографической защиты информации

1. Определение криптографической системы, виды криптосистем.
2. Базовые криптографические примитивы. Шифры перестановки и замены.
3. Блочные и поточные шифры.
4. Вычислительно сложные задачи и однонаправленные функции, используемые в криптографии.
5. Модели шифров. Основные требования к шифрам. Совершенные шифры, криптографические хеш-функции.

6. Криптографические параметры узлов и блоков шифраторов. Синтез шифров.
7. Методы получения случайных и псевдослучайных последовательностей; программные реализации шифров.
8. Суть криптографических методов защиты информации (ЗИ). Основные задачи по ЗИ, решаемые с использованием криптографических методов. Значение криптографических методов в комплексной системе ЗИ. Базовые понятия криптологии (шифр, ключи, протоколы, шифрсистема).
9. Криптографическая стойкость шифров. Активные и пассивные атаки на шифрсистемы, задачи криптоаналитика. Теоретически стойкие шифры. Практическая стойкость шифров, её основные характеристики (трудоёмкость и надёжность дешифрования, количество необходимого материала).
10. Классификация шифрсистем с секретным ключом. Шифрсистемы поточного шифрования (синхронные и асинхронные).
11. Системный подход к построению практически стойких шифров. Характеристики случайности и непредсказуемости выходных последовательностей генераторов (периодичность, линейная сложность, статистические характеристики).
12. Криптография с открытым ключом. Основные принципы. Сравнение криптосистем с открытым и секретным ключом.

Основы защиты информации от утечки по техническим каналам

1. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Опасные сигналы и их источники.
2. Структура, классификация и основные характеристики технических каналов утечки информации. Основные методы и средства защиты информации от утечки по техническим каналам.
3. Технические каналы утечки акустической (речевой) информации. Основные характеристики. Основные методы и средства защиты речевой информации в помещениях.
4. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов.
5. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей.
6. Экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания.
7. Технические каналы утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Основные характеристики. Основные методы и средства защиты информации от утечки за счет ПЭМИН.

8. Технические каналы утечки информации при передаче по каналам связи. Основные характеристики. Основные методы и средства защиты информации в каналах связи.
9. Технические каналы утечки информации средств вычислительной техники. Основные характеристики.
10. Построение модели технических каналов утечки информации и оценка возможностей нарушителя по их использованию.

Программно-аппаратные методы защиты информации от несанкционированного доступа

1. Основные принципы создания программно-аппаратных средств защиты информации. Концепция диспетчера доступа.
2. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение.
3. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности. Построение изолированной программной среды.
4. Программно-аппаратные средства защиты информации в сетях передачи данных.
5. Организация управления доступом и защиты ресурсов ОС. Основные механизмы безопасности: средства и методы аутентификации в ОС.
6. Модели разграничения прав доступа, организация и использование средств аудита.
7. Методы идентификации и аутентификации. Общая характеристика функции аутентификации.
8. Методы реализации контроля и разграничения прав доступа. Функции контроля и разграничения прав доступа.
9. Модель нарушителя доступа при защите автоматизированных систем от несанкционированного доступа.
10. Методы контроля защищенности автоматизированных систем от несанкционированного доступа.

Защита информации от вредоносного программного обеспечения.

1. Общее описание компьютерных вирусов. Видовая классификация компьютерных вирусов.
2. Методы и средства антивирусной защиты.
3. Организационно-правовые методы защиты от вирусов
4. Защита от вирусов в статике процессов.

5. Защита от вирусов в динамике процессов.
6. Антивирусная политика на объекте информатизации.
7. Основные направления антивирусной борьбы в компьютерных и телекоммуникационных системах.
8. Основные механизмы внедрения компьютерных вирусов в поражаемую систему.

ЛИТЕРАТУРА ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

Основная литература

1. Информационная безопасность: концептуальные и методологические основы защиты информации / Малюк А.А. – М. Горячая линия-Телеком, 2004. – 280 с.
2. Кудряшов Б.Д. Теория информации. Учебник для вузов. – СПб.: Питер, 2009. – 320 с.
3. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - М. Горячая линия-Телеком, 2014. – 244 с.
4. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: (Высшее образование) ISBN 978-5-369-01450-9.
5. Шустова Лариса Ивановна Шустова Л.И. Базы данных: учебник / Л.И. Шустова, О.В. Тараканов. — М.: ИНФРА-М, 2017. — 304 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/11549.
6. Комплексная система защиты информации на предприятии / Грибунин В.Г - М.: Академия, 2009.
7. Математические и компьютерные основы криптологии / Харин Ю.С.- М.: Новое знание, 2008.
8. Фомичёв В. М., Мельников Д.А. Криптографические методы защиты информации в 2 ч.: учебник для вузов / под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2022. — 245 с.
9. Запечников С.В. Криптографические методы защиты информации. Учебное пособие. Запечников С.В., Казарин О.В., Тарасов А.А. – Москва: Юрайт Москва, 2015. – 309 с.
10. Запечников С.В. Основы построения виртуальных частных сетей: учеб. пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. – М.: Горячая линия–Телеком, 2003. – 249 с.
11. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2011. – 320 с.

12. Мельников Д.А. Информационная безопасность открытых систем. Учебник. – М: Флинта, Наука, 2013. – 448 с.
13. Основы защиты информации: Учебное пособие / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов. -М.: Издательский центр «Академия», 2006.
14. Защита информации в телекоммуникационных системах / Коханович Г.Ф. и др. - М.: Пресс, 2005.
15. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: Машиностроение, 2009. — 508 с.
16. Борисов М.А. Основы организационно-правовой защиты информации. Борисов М.А., Романов О.А. – М: Ленанд, 2015. – 248 с.
17. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.

Дополнительная литература

1. Безопасность глобальных сетевых технологий / Игнатов В.Г. - СПб.: Питер, 2007.
2. Методы и средства защиты информации в компьютерных системах / Хорев П.Б. - М.: Академия, 2006.
3. Защита информации в системах мобильной связи / Чекалин А. А.- М.: Горячая линия- Телеком, 2005.
4. Дискретная математика и криптология / Фомичев В.М.. 2-е изд. -М,: ДИАЛОГ-МИФИ, 2009.
5. Комплексная защита информации в корпоративных системах / Шаньгин В.Ф. - М.: ИД Форум: НИЦ Инфра-М, 2012.
6. Информационная безопасность / Ярочкин В. И. - М.: Академия - проспект, 2006.
7. Основы информационной безопасности / Белов Е.Б. - М.: Горячая линия-Телеком, 2006.
8. Защита компьютерной информации от несанкционированного доступа / Щеглов Ю.А. - М.: Наука и техника, 2004.
9. Теоретико-числовые методы в криптографии / Маховенко Е.Б. - М.: Гелиос, 2006
10.. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации (Учебное пособие) / Горбатов В.С., Дворянкин С.В., Дураковский А.П., Енгалычев Р.С. и др. Под общей редакцией Лаврухина Ю.Н. - М: НИЯУ МИФИ, 2014. -560 с.
11. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем. Учебник. – М: Университетская книга, 2012. – 598 с.

3. Материалы для подготовки ко второй части вступительного испытания

При представлении плана научного исследования необходимо представить следующую информацию:

- Тема диссертации
- Предполагаемый научный руководитель (при наличии)
- Актуальность темы
- Цели и задачи исследования
- Развернутые формулировки теоретических и практических задач, которые необходимо решить для достижения поставленной цели с распределением их по семестрам обучения.
- Теоретическая значимость работы. Практическая значимость работы.
- Имеющийся задел по предполагаемому исследованию

Абитуриент готовит план будущего научного исследования заранее, до вступительного испытания, и на испытании представляет уже готовый план. При составлении плана необходимо помнить, что в рамках диссертационного исследования аспирант решает научную задачу, имеющую значение для развития соответствующей отрасли науки, либо разрабатывает новые научно-обоснованные технические, технологические или иные решения и разработки, имеющие существенное значение для развития страны.

Цель диссертации вытекает из формулировки научной проблемы, связанной с теоретической или практической нерешенностью темы или ее аспекта. Цель формулируется коротко и однозначно, она должна быть достигнута к концу работы. Исходя из единственной цели работы, определяется несколько задач. Разрешение каждой задачи является последовательным шагом на пути достижения цели.

Паспорт научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность». (отрасль наук – физико-математические науки, технические науки):

Направления исследований:

1. Теория и методология обеспечения информационной безопасности и защиты информации.
2. Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
3. Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.
4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.

5. Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
7. Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.
8. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.
9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.
10. Модели и методы оценки защищенности информации и информационной безопасности объекта.
11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.
12. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
13. Методы и модели выявления и противодействия распространению ложной и вредоносной информации.
14. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
16. Модели, методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.
17. Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях.
18. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.
19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.