МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
Московский государственный университет геодезии и картографии (МИИГАиК)

Утверждаю:
Проректор
_____ А.Л. Степанченко
«19» 01 2026 г.

ПРОГРАММА

вступительного испытания для поступающих на обучение по программам подготовки научных и научно-педагогических кадров в аспирантуре

Научная специальность: **2.3.6 Методы и системы защиты информации, информационная безопасность**

МОСКВА 2026

Программа вступительного испытания составлена на основании Федеральных государственных образовательных стандартов высшего образования по программам специалитета и магистратуры.

И.о. директора института инфокоммуникационных систем и технологий

_____канд. техн. наук, с.н.с. И.В. Парафейников

Зав. кафедрой Информационной безопасности

_____канд. техн. наук, доцент С.Ю. Сазонов

Введение

Вступительное испытание по специальной дисциплине, соответствующей научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность проводится в устной форме.

Экзаменационные билеты состоят из трех вопросов.

Критерии оценки знаний и умений поступающего в аспирантуру

При принятии экзамена необходимо иметь в виду следующие критерии:

- знание учебного материала предмета (учебной дисциплины);
- наличие аналитического мышления;
- владение категориальным аппаратом;
- общий (культурный) и специальный (профессиональный) язык ответа.

Каждый вопрос экзаменационного билета оценивается комиссией раздельно, по 100-балльной шкале. Итоговая оценка за вступительное испытание определяется как среднее арифметическое. Неудовлетворительная оценка за экзамен в целом установлена в диапазоне от 0 до 39.

Баллы	Критерии выставления оценки
90-100	Оценка ставится при полных, исчерпывающих, аргументированных ответах на все основные и дополнительные экзаменационные вопросы. Ответы должны отличаться логической последовательностью, четкостью в выражении мыслей и обоснованностью выводов, демонстрирующих знание источников, понятийного аппарата и умения ими пользоваться при ответе.
78-89	Оценка ставится при достаточно полных и аргументированных ответах на все основные и дополнительные экзаменационные вопросы. Ответы должны отличаться логичностью, четкостью, знанием понятийного аппарата и литературы по теме вопроса при незначительных упущениях при ответах.
65-77	Оценка ставится за в целом достаточное знание рассматриваемого вопроса, но с отдельными заметными ошибками.
52-64	Оценка ставится при неполных и слабо аргументированных ответах, демонстрирующих общее представление и элементарное понимание существа поставленных вопросов, понятийного аппарата и обязательной литературы.
40-51	Оценка ставится за самое общее представление о рассматриваемом вопросе, отвечающее лишь минимальным требованиям.
0-39	Оценка ставится при незнании и непонимании поступающим существа экзаменационных вопросов.

ПРОГРАММА ЭКЗАМЕНА

Раздел 1. Теоретические основы защиты информации

Основные свойства информации как предмета защиты. Количество информации. Основные свойства информации, влияющие на возможность ее защиты.

Проблема защиты информации. Современное состояние защиты информации, перспектива и ретроспектива. Информационные системы, средства, каналы, сети и среды.

Основные положения теории защиты информации. Определение и основные понятия теории защиты информации. Общеметодологические принципы формирования теории защиты информации. Стратегии защиты информации.

Угрозы безопасности информации. Информационные угрозы. Информационные атаки.

Политика безопасности. Процесс разработки политики. Неформальное описание политики безопасности. Формальное описание политики безопасности.

Дискреционный контроль и управление доступом. Матрица доступа. Модель Харрисона, Руззо и Ульмана. Модель распространения прав доступа TAKE-GRANT.

Модель распространения прав доступа take-grant. Санкционированное получение прав доступа. Похищение прав доступа. Расширенная модель TakeGrant.

Модели мандатного контроля и управления доступом. Уровни секретности. Модель Белла и Лападула. Критика модели Белла и Лападула.

Модели контроля целостности. Модель Биба. Модель Кларка-Вилсона. Объединение моделей безопасности. Объединение модели Белла и Лападула и модели Биба. Объединение моделей Кларка—Вилсона и Биба. Модель Липнера. Модель Липнера на основе модели Белла и Лападула и Биба.

Ролевые модели доступа. Пользователи, роли и операции. Роли и иерархия ролей. Авторизация и активация роли. Операционное разделение обязанностей и доступ к объектам.

Идентификация и аутентификация. Роль и задачи аутентификации. Парольная аутентификация. Биометрическая аутентификация. Аутентификация, основанная на обладании предметом.

Аудит информационной безопасности. Требования к подсистеме аудита. Реализация подсистемы аудита в операционной системе Windows. Аудит информационной безопасности предприятия.

Уязвимости. Основные определения. Ошибки, приводящие к уязвимостям. Поиск уязвимостей в процессе разработки и анализа систем.

Атаки и вторжения. Характеристики атак. Вторжения. Компьютерные вирусы и черви. Поиск уязвимостей в процессе функционирования систем.

Раздел 2. Криптографические основы защиты информации

Криптография как способ реализации сервисов безопасности. Классификация шифров. Общая классификация шифров.

Криптографическая стойкость шифров. Понятия стойкости. Формальные модели атак. Теоретико-информационный подход. Теоретико-сложностной подход.

Математические модели шифров. Алгебраическая модель шифра. Вероятностная модель шифра. Автоматная модель шифра.

Математические модели открытых текстов. Детерминированные модели. Вероятностные модели.

Основные алгоритмы симметричного шифрования. Стандарт шифрования DES. Стандарт шифрования AES. Российский стандарт криптографической защиты информации ГОСТ 28147-89.

Режимы использования блочных шифров. Режим электронной кодовой книги. Режим сцепления блоков зашифрованного текста. Режим обратной связи по зашифрованному тексту. Режим обратной связи по выходу. Режим счетчика.

Алгоритмы поточного шифрования.

Методы получения случайных и псевдослучайных последовательностей. Физические генераторы случайных чисел. Табличные генераторы случайных чисел. Алгоритмические генераторы случайных чисел.

Асимметричные шифры.

Алгоритмы шифрования с открытым ключом. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Меркла-Хеллмана Криптосистема Рабина. Принципы шифрования с использованием эллиптических кривых.

Раздел 3. Техническая защита информации

Государственная система защиты информации. Основные направления защиты информации. Цели и задачи защиты информации от утечки информации по техническим каналам. Объекты технической защиты информации. Нормативные документы по технической защите информации. Объект информатизации (определение и характеристика). Характеристика основных технических средств и систем. Характеристика вспомогательных технических средств и систем.

Технические каналы утечки информации Структура и состав технического канала утечки информации. Классификация технических каналов утечки информации. Основные показатели технических каналов утечки информации.

Концепция технической защиты информации. Общие принципы технической защиты информации. Принципы построения системы защиты информации. Классификация направлений и методов защиты. Характеристика методов скрытия информации.

Виды сообщений в информационно-телекоммуникационных системах. Классификация сигналов. Сравнительная характеристика аналоговых и дискретных сигналов. Временное и спектральное представление сигналов. Принципы записи информации на носители в виде физических полей. Виды модуляции. Характеристика аналоговых видов модуляции. Характеристика импульсных видов модуляции (манипуляции). Принципы передачи и считывания информации с носителей в виде физических полей.

Определения угроз безопасности информации информационных систем и субъектов информационных отношений. Источники угроз безопасности информационных систем, их классификация. Основные непреднамеренные искусственные угрозы информационных систем. Основные преднамеренные искусственные угрозы информационных систем.

Доступ к информации, условия разведывательного контакта. Способы и каналы несанкционированного доступа к информации. Опасные случайные сигналы и их источники.

Паразитные связи и наводки как источники опасных сигналов. Низкочастотные и высокочастотные излучения технических средств.

Техническая разведка. Классификация и характеристика видов технической разведки. Классификация и характеристика технических средств разведки. Возможности (показатели) технической разведки и ее средств.

Общая характеристика радиоэлектронных технических каналов утечки информации. Классификация радиоэлектронных технических каналов утечки информации. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений | (ПЭМИ). Структура и характеристика электромагнитного технического канала утечки информации. Характеристика сигналов ПЭМИ от средств вычислительной техники. Перехват побочных электромагнитных излучений средств вычислительной техники. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Перехват наведенных информационных сигналов. Технический канал утечки информации, создаваемый путем высокочастотного облучения.

Общая характеристика речевого сигнала. Линейные характеристики акустического поля. Энергетические характеристики акустического поля. Фонетические характеристики речи.

Способы перехвата акустической (речевой) информации Классификация способов перехвата акустической (речевой) информации. Схема и характеристика прямого акустического канала перехвата речевой информации. Схемы каналов перехвата речевой информации с использованием микрофонов и диктофонов. Схемы каналов перехвата речевой информации с использованием закладных устройств с передачей информации по каналам связи. Схема перехвата речевой информации с использованием устройств типа «телефонное ухо» с передачей информации по телефонной линии на низкой частоте.

Способы перехвата информации, передаваемой по каналам проводной связи. Схема перехвата информации, передаваемой по телефонному каналу. Схемы подключения закладных устройств к телефонной линии. Перехват данных, передаваемых по телефонной линии в сети Интернет.

Способы перехвата информации, передаваемой по каналам радиосвязи. Структура и характеристика комплекса средств перехвата информации, передаваемой по радиоканалу. Характеристика сетей подвижной радиосвязи общего пользования как объектов защиты. Перехват информации в сетях сотовой и транкинговой связи. Перехват информации, передаваемой с использованием радиотелефонов. Перехват информации, передаваемой в сетях беспроводного доступа.

Классификация методов и средств защиты информации от утечки по техническим каналам.

Способы экранирования, их характеристики. Требования к различным видам экранов. Экранирование технических средств. Экранирование соединительных линий. Экранирование помещений.

Заземление технических средств. Схемы заземления. Основные требования, предъявляемые к системе заземления. Заземление технических средств. Сопротивление заземления. Заземление технических средств. Характеристика средств заземления.

ЛИТЕРАТУРА

1. Баланов А. Н. Кибербезопасность : учебное пособие / А. Н. Баланов. - Санкт-Петербург : Издательство «Лань», 2026. - 460 с. - ISBN 978-5-534-18246-7.
2. Баланов А. Н. Криптографические основы защиты информации: учебное пособие / А. Н. Баланов. - Санкт-Петербург: Издательство «Лань», 2026. - 460 с. - ISBN 978-5-534-18246-7.
3. Баранова Е. К., Бабаш А. В. Криптографические методы защиты информации: учебник / Е. К. Баранова, А. В. Бабаш. - Электронное издание. - Москва: Издательство «Юрайт», 2026.
4. Белов А. С., Добрышин М. М. Системный подход к проектированию систем обеспечения информационной безопасности / А. С. Белов, М. М. Добрышин. - Москва: Издательство «Юрайт», 2023. - ISBN 978-5-534-16481-6.
5. Бубнов А. А. Техническая защита информации в объектах информационной инфраструктуры / А. А. Бубнов. - Ставрополь: Академия, 2019.
6. Васильева И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Издательство «Юрайт», 2024. - 432 с. - ISBN 978-5-534-16478-6.
7. Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - Санкт-Петербург : Издательство «Лань», 2026. - 1529 с. - ISBN 978-5-534-18247-4.
8. Жданов О. Н., Чалкин В. А. Эллиптические кривые: основы теории и криптографические приложения / О. Н. Жданов, В. А. Чалкин. - Электронное издание. - Москва: Издательство «Юрайт», 2026.
9. Зайцев А. П., Мещеряков Р. В., Шелупанов А. А. Технические средства и методы защиты информации: учебник для вузов / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. - Москва: Горячая Линия - Телеком, 2024. - ISBN 978-5-93517-192-7.
10. Запонов Э. В., Мартынов А. П., Машин И. Г. и др. Методы и средства комплексной защиты информации в технических системах: учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин и др. - Саров: РФЯЦ-ВНИИЭФ, 2019. - ISBN 978-5-9515-0429-6.
11. Калашников А. О., Аникина Е. В., Остапенко Г. А., Борисов В. И. Влияние новых технологий на информационную безопасность критической информационной инфраструктуры // Информация и безопасность. - 2019. - Т. 22, вып. 2. - С. 156–169.
12. Калашников А. О., Бугайский К. А., Аникина Е. В. Модели количественного оценивания компьютерных атак (часть 2) // Информация и безопасность. - 2019. - Т. 22, вып. 4. - С. 529–538.

13. Калашников А. О., Максимовский А. Ю. Использование специальных соотношений в автоматах для мониторинга информационной безопасности сетевых объектов // Информация и безопасность. - 2019. - Т. 22, вып. 1. - С. 30–37.

14. Калашников А. О., Максимовский А. Ю. Развитие автоматных моделей мониторинга информационной безопасности сетевых объектов // Информация и безопасность. - 2019. - Т. 22, вып. 4. - С. 549–556.

15. Котов Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом / Ю. А. Котов. - Электронное издание. - Москва: Издательство «Юрайт», 2026.

16. Котов Ю. А. Криптографические методы защиты информации. Шифры / Ю. А. Котов. - Электронное издание. - Москва: Издательство «Юрайт», 2026.

17. Краковский Ю. М. Методы и средства защиты информации / Ю. М. Краковский. - Санкт-Петербург: Издательство «Лань», 2025. - ISBN 978-5-534-18252-8.

18. Крамаров С. О., Тищенко Е. Н., Соколов С. В. и др. Криптографическая защита информации: учебное пособие / С. О. Крамаров, Е. Н. Тищенко, С. В. Соколов и др. - Москва: ИЦ РИОР, 2026. - 323 с. - ISBN 978-5-369-01716-6.

19. Лозовецкий В. В., Комаров Е. Г. Комплексное обеспечение информационной безопасности на предприятии: учебник / В. В. Лозовецкий, Е. Г. Комаров. - Санкт-Петербург: Издательство «Лань», 2025. - ISBN 978-5-534-18255-9.

20. Малюк А. А. Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов. - Москва : Издательство «Юрайт», 2023. - 224 с. - ISBN 978-5-534-16477-9.

21. Мельников Д. А. Информационная безопасность открытых систем. В 2 т. Т. 2. Средства защиты в сетях / Д. А. Мельников. - Москва: Издательство «Юрайт», 2023. - ISBN 978-5-534-16482-3.

22. Мельников Д. А., Фомичев В. М. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / Д. А. Мельников, В. М. Фомичев. - Электронное издание. - Москва: Издательство «Юрайт», 2026.

23. Мельников Д. А., Фомичев В. М. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / Д. А. Мельников, В. М. Фомичев. - Электронное издание. - Москва: Издательство «Юрайт», 2026.

24. Нестеренко А. Ю., Лось А. Б., Рожков М. И. Криптографические методы защиты информации: учебник / А. Ю. Нестеренко, А. Б. Лось, М. И. Рожков. - 2-е изд. - Москва: Издательство «Юрайт», 2019. - 473 с..

25. Никифоров С. Н. Методы защиты информации. Защищённые сети: учебное пособие / С. Н. Никифоров. - Санкт-Петербург: Издательство «Лань», 2026. - ISBN 978-5-534-18254-2.

26. Петренко В. И., Мандрица И. В. Практикум по дисциплине «Технические средства и методы защиты информации»: учебное пособие / В. И. Петренко, И. В. Мандрица. - Санкт-Петербург: Издательство «Лань», 2026. - ISBN 978-5-534-18253-5.

27. Прокушев Я. Е. Информационная безопасность операционных систем Linux: практикум по защите информации / Я. Е. Прокушев. - Москва: Издательство «Юрайт», 2023. - ISBN 978-5-534-16480-9.

28. Прохорова О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. - Санкт-Петербурга : Издательство «Лань», 2026. - 507 с. - ISBN 978-5-534-18248-1.

29. Рацеев С. М. Криптографические методы защиты информации и их основы. Лабораторный практикум : учебное пособие / С. М. Рацеев. - Санкт-Петербург : Издательство «Лань», 2026. - 1134 с. - ISBN 978-5-534-18249-8.

30. Рацеев С. М. Основы криптографии на решётках : учебное пособие / С. М. Рацеев. - Санкт-Петербург : Издательство «Лань», 2026. - 1513 с. - ISBN 978-5-534-18250-4.

31. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. - Электронное издание. - Москва: Издательство «Юрайт», 2026.
32. Сидак А. Е., Василенко В. В., Рыженко С. В. Информационная безопасность. Физические основы технических каналов утечки информации / А. Е. Сидак, В. В. Василенко, С. В. Рыженко. - Москва: Директ-Медиа, 2022. - ISBN 978-5-4475-1824-7.
33. Тарасов А. А., Казарин О. В., Запечников С. В. Криптографические методы защиты информации: учебник / А. А. Тарасов, О. В. Казарин, С. В. Запечников. - Москва: Издательство «Юрайт», 2019. - 309 с..
34. Тумбинская М. В., Петровский М. В. Защита информации на предприятии / М. В. Тумбинская, М. В. Петровский. - Санкт-Петербург: Издательство «Лань», 2025. - ISBN 978-5-534-18251-1.
35. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. - Москва: Издательство «Юрайт», 2023. - ISBN 978-5-534-16479-3.

Internet-ресурсы (в т.ч. перечень мировых библиотечных ресурсов, видеоролики и видеоконференции):

1. http://www.rsl.ru/ (Российская государственная библиотека);
2. http://www.gpntb.ru/ (Государственная публичная научно-техническая библиотека России);
3. https://fstec.ru/ (официальный сайт Федеральной службы по техническому и экспортному контролю);
4. https://rkn.gov.ru/ (официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор));
5. http://www.fsb.ru/ (официальный сайт Федеральной службы безопасности Российской Федерации);
6. http://www.consultant.ru/ (Консультант Плюс - законодательство РФ кодексы и законы в последней редакции);
7. http://www.iso27000.ru/ (Интернет портал Защита-информации.SU);
8. https://www.biblioclub.ru/ (ЭБС «Университетская библиотека ОНЛАЙН»);
9. https://www.iprbookshop.ru/ (ЭБС IPR SMART);
10. https://znanium.com/ (ЭБС Znanium);
11. http://www.rfbr.ru/ (Российский фонд фундаментальных исследований);
12. http://dic.academic.ru (Словари и энциклопедии);
13. http://elibrary.ru (Научная электронная библиотека);
14. http://www.library.ru (Виртуальная справочная служба);
15. http://www.nlr.ru (Российская национальная библиотека);
16. http://www.ribk.net (Российский информационно-библиотечный консорциум);
17. https://e.lanbook.com/ (Электронная библиотека Лань).