МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ
УНИВЕРСИТЕТ (РИНХ)»

УТВЕРЖДАЮ
Председатель Приемной комиссии,
ректор ФГБОУ ВО «РГЭУ (РИНХ)»
д.э.н., профессор
_____ Е.Н. Макаренко
«__» _____2023 г.

ПРОГРАММА
ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ
В АСПИРАНТУРУ ФГБОУ ВО «РГЭУ (РИНХ)»
на 2024/2025 учебный год

Ростов–на–Дону – 2023

ПРОГРАММА
ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ В АСПИРАНТУРУ
по специальной дисциплине

Научная специальность 2.3.6. Методы и системы защиты информации, информационная безопасность

СТРУКТУРА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ В АСПИРАНТУРУ

Программа вступительного испытания предназначена для поступающих на образовательные программы высшего образования – программы подготовки научных и научно-педагогических кадров в аспирантуре.

Программа вступительного испытания сформирована на основе федеральных государственных образовательных стандартов по программам магистратуры 10.04.01 Информационная безопасность.

Цель вступительного испытания – выявление среди поступающих наиболее способных и подготовленных к освоению образовательной программы высшего образования – программы подготовки научных и научно-педагогических кадров в аспирантуре.

Вступительное испытание проводится в устной форме по экзаменационным билетам. Экзаменационный билет содержит три вопроса.

Вступительное испытание проводится на русском языке. Поступающий однократно сдает вступительное испытание.

Во время экзамена абитуриентам запрещается пользоваться мобильными телефонами и любым другим электронным оборудованием.

ПЕРЕЧЕНЬ ВОПРОСОВ

1. Стратегические цели и основные направления обеспечения информационной безопасности РФ.
2. Законодательно – правовые и организационные основы обеспечения защиты информации.
3. Организация защиты информации на предприятии.
4. Выбор показателей эффективности и критериев оптимальности комплексной системы защиты информации.
5. Моделирование комплексной системы защиты информации.
6. Политика безопасности предприятия.
7. Синтез системы защиты информации. Разработка технического задания.
8. Структура системы государственного лицензирования.
9. Лицензионные требования и условия в области защиты информации.
10. Структура системы сертификации в области защиты информации.
11. Порядок сертификации средств защиты информации.
12. Порядок проведения аттестации объектов информатизации.
13. Аттестация объектов информатизации. Подготовка исходных данных.
14. Аттестация объектов информатизации. Оформление результатов аттестации.
15. Законодательство РФ о государственной тайне. Полномочия органов

государственной власти и должностных лиц.

16. Порядок засекречивания и рассекречивания сведений и их носителей.
17. Порядок допуска к государственной тайне.
18. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности.
19. Организация допуска должностных лиц и граждан к государственной тайне.
20. Организация и порядок проведения специальных экспертиз предприятий.
21. Коммерческая тайна как вид защищаемой конфиденциальной информации.
22. Охрана коммерческой тайны в рамках трудовых отношений.
23. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
24. Состав и структура системы безопасности предприятия.
25. Правовые основы деятельности службы безопасности.
26. Силы и средства, используемые при организации внутриобъектового режима.
27. Основные элементы системы организации пропускного режима.
28. Оценка и управление рисками. Экономическая оценка систем и средств защиты.
29. Технические методы и средства защиты информации от утечки по техническим каналам.
30. Методы защиты информации от несанкционированного доступа.
31. Обеспечение информационной безопасности при вводе объектов в эксплуатацию.
32. Выбор и оптимизация требуемых средств защиты информации на объектах.
33. Классификация методов зашиты информации от программно-математических воздействий.
34. Деятельность администратора безопасности по предотвращению программно-математических воздействий.
35. Формирование требований к защите информации в информационной системе.
36. Определение класса защищенности информационной системы.
37. Требования к мерам защиты информации в информационной системе.
38. Модель угроз безопасности информации в информационной системе.
39. Модель нарушителя в информационной системе.
40. Аттестация информационной системы и ввод ее в действие.
41. Аудит состояния информационной безопасности на объектах информатизации.
42. Методы экспертного анализа состояния информационной безопасности на объектах информатизации.
43. Виды контроля состояния информационной безопасности объектов.
44. Объектовый мониторинг состояния информационной безопасности.
45. Формы представления результатов контроля информационной безопасности.
46. Методы оценки эффективности мероприятий информационной безопасности.

47. Расчетно-аналитические методы оценки эффективности систем информационной безопасности.

48. Средства управления безопасностью локальных сетей.

49. Аппаратная защита электронного обмена информацией

50. Нормативно-правовое обеспечение защиты персональных данных.

51. Требования к защите персональных данных при их обработке в ИСПДн.

52. Принципы и условия обработки ПДн. Обязанности оператора ПДн.

53. Порядок организации защиты ПДн. Состав и содержание мер по обеспечению безопасности ПДн.

54. Основные положения базовой модели угроз безопасности ПДн при их обработке в ИСПДн.

55. Законодательно-правовые акты, регулирующие деятельность по организации защиты объектов КИИ.

56. Порядок формирования перечня объектов КИИ.

57. Основные этапы категорирования объектов КИИ.

58. Техническая реализация аппаратных средств защиты информации

59. Архитектура семейства технических устройств аппаратной защиты информации

60. Управление рисками. Модель безопасности с полным перекрытием

61. Современные стандарты в области информационной безопасности, использующие концепцию управление рисками.

62. Основные направления использования современной криптографии.

63. Основные требования к криптосистемам.

64. Классификация методов криптографического преобразования информации.

65. Структура алгоритма DES. Анализ особенностей блоков начальной и заключительной перестановок.

66. Принцип построения схемы шифрования с открытым ключом.

67. Принцип построения схемы электронной цифровой подписи.

68. Практическая стойкость криптосистемы и параметры, ее характеризующие.

69. Структура алгоритма шифрования RSA. Условия его работоспособности и их теоретическое обоснование.

70. Организация криптосистем на основе канального и сквозного шифрования. Основные преимущества и недостатки обоих типов шифрования.

71. Преступления в сфере компьютерной информации. Признаки и элементы состава преступления.

ШКАЛА ОЦЕНИВАНИЯ
И КРИТЕРИИ ОЦЕНКИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Уровень знаний поступающего в аспирантуру оценивается экзаменационной комиссией по 100-балльной системе.

Максимальное количество баллов, которое поступающий может получить на вступительном испытании, равно 100 баллам. Минимальное количество баллов, подтверждающее успешное прохождение поступающим вступительного испытания, составляет 50 баллов.

Критерии оценивания ответов поступающего в аспирантуру на экзаменационные вопросы по специальной дисциплине:

Баллы	**Критерии оценивания**
84 - 100	поступающий исчерпывающе, логически и аргументированно излагает материал, демонстрирует наличие глубоких исчерпывающих знаний в объеме программы вступительного испытания; обосновывает собственную точку зрения при анализе конкретной проблемы исследования, свободно отвечает на поставленные дополнительные вопросы, делает обоснованные выводы
67 - 83	баллов выставляется, если поступающий демонстрирует наличии твердых и достаточно полных знаний в объеме программы вступительного испытания, проявляет логичность и доказательность изложения материала, но допускает отдельные неточности при использовании ключевых понятий; в ответах на дополнительные вопросы имеются незначительные ошибки
50 - 66	поступающий поверхностно раскрывает основные теоретические положения программы вступительного испытания, у него имеются базовые знания специальной терминологии, но в усвоении материала имеются пробелы, излагаемый материал не систематизирован; выводы недостаточно аргументированы, имеются смысловые и речевые ошибки
0 - 49	поступающий допускает фактические ошибки и неточности в области основных теоретических положений, изложенных в программе вступительного испытания, у поступающего отсутствуют знания специальной терминологии, нарушена логика и последовательность изложения материала; поступающий не отвечает на дополнительные вопросы по рассматриваемым темам, не может сформулировать собственную точку зрения по обсуждаемому вопросу