

Министерство транспорта Российской Федерации
Федеральное агентство железнодорожного транспорта
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Дальневосточный государственный университет путей сообщения»
(ДВГУПС)

УТВЕРЖДАЮ

Председатель приемной
комиссии ДВГУПС, ректор

В.В.Буровцев
2025 г.



ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ
по подготовке научных и научно-педагогических кадров в аспирантуре

научная специальность – 1.2.4 Кибербезопасность

Хабаровск
2025

СОДЕРЖАНИЕ ПРОГРАММЫ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

1. Общие положения.
2. Цели и задачи программы вступительных испытаний.
3. Структура программы:
 - 3.1. Требования к вступительному испытанию.
 - 3.2. Тематическое содержание.
 - 3.3. Перечень вопросов для вступительного испытания.
 - 3.4. Критерии оценивания результата вступительного испытания.
4. Список рекомендуемой литературы.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и область применения

Настоящая программа составлена в соответствии с паспортом научной специальности 1.2.4 «Кибербезопасность» и определяет содержание и форму вступительного испытания по указанному направлению.

2. ЦЕЛИ И ЗАДАЧИ ПРОГРАММЫ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

Цель вступительных испытаний состоит в том, чтобы определить готовность экзаменуемого к обучению по программе подготовки научных и научно-педагогических кадров в аспирантуре по научной специальности 1.2.4 «Кибербезопасность».

Задачей программы вступительных испытаний является оценка степени и уровня знаний поступающих на программы подготовки научных и научно-педагогических кадров в аспирантуре, характеризующая их подготовленность к самостоятельному выполнению определенных видов профессиональной деятельности; определение объема и содержания профессиональных знаний, методических и практических умений, аналитических способностей и профессионального мышления аспирантов.

3. СТРУКТУРА ПРОГРАММЫ

3.1. Требования к вступительному испытанию

Для поступающих на места в рамках контрольных цифр приема, а также по договорам об оказании платных образовательных услуг на определенную научную специальность устанавливается одно вступительное испытание - специальная дисциплина, соответствующая научной специальности программы подготовки научных и научно-педагогических кадров в аспирантуре (далее – специальная дисциплина).

Вступительное испытание проводится в письменной форме по экзаменационным билетам.

Вступительное испытание проводится на русском языке.

Билет содержит три вопроса (задания).

Максимальное количество баллов, полученных за ответы на 3 вопроса, составляет 100 баллов.

Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания составляет 45 баллов.

Результаты проведения вступительного испытания оформляются протоколами. На каждого поступающего ведется отдельный протокол.

Протоколы приема вступительных испытаний и экзаменационные листы ответов письменной формы экзамена после утверждения хранятся в личном деле поступающего.

3.2. Тематическое содержание

В программе рассматриваются следующие разделы:

Раздел 1. Организационные основы информационной безопасности

Основные понятия и принципы теории информационной безопасности. Угрозы информационной безопасности, их анализ. Виды информации, методы и средства обеспечения информационной безопасности. Методы нарушения конфиденциальности, целостности и доступности информации.

Основы комплексного обеспечения информационной безопасности. Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Лицензирование и сертификация в области защиты информации.

Правовые основы защиты информации с использованием технических средств. Защита интеллектуальной собственности. Основы законодательства в области защиты информации.

Раздел 2. Избранные разделы математики

Основные понятия теории вероятностей. Случайные события и случайные величины. Основные законы распределения случайных величин. Математическое ожидание и дисперсия. Многомерные случайные величины. Многомерное нормальное распределение. Гауссовский случайный процесс с дискретным и непрерывным временем. Понятие стационарности процесса. Марковские процессы и цепи. Понятия стационарности и эргодичности случайного процесса. Классификация марковских цепей и их состояний. Уравнения Колмогорова для переходных вероятностей марковского процесса. Предельные вероятности. Процессы с независимыми приращениями. Теорема о свойствах его конечномерных распределений. Основные модели процессов с независимыми приращениями: пуассоновский, сложный пуассоновский и винеровский процессы. Теория систем массового обслуживания. Система массового обслуживания без очереди и с очередью.

Комбинаторные задачи и основные принципы комбинаторики. Перестановки и подстановки. Размещения и сочетания без повторений. Размещения и сочетания с повторениями.

Матрицы. Виды матриц. Линейные операции над матрицами. Произведение матриц. Элементарные преобразования матриц. Обратная матрица и ее вычисление с помощью элементарных преобразований и методом Крамера. Геометрический вектор, Равенство векторов, коллинеарность и компланарность. Линейные операции над векторами. Линейная зависимость. Базис. Декартов базис. Скалярное произведение векторов, его свойства, вычисление. Векторное произведение векторов и его свойства.

Бесконечная числовая последовательность и ее предел. Теория пределов. Непрерывность. Классификация разрывов. Дифференцирование функции одной переменной. Основные теоремы дифференциального исчисления. Исследование функции одной переменной. Неопределенный интеграл, Определение и существование. Свойства. Приемы интегрирования. Определенный интеграл Римана. Несобственные интегралы.

Числовые ряды. Признаки сходимости. Знакопеременные ряды. Абсолютная и условная сходимость. Степенные ряды. Радиус сходимости. Ряд Тейлора. Разложение основных функций в степенной ряд. Ряд Фурье. Условия сходимости. Интеграл Фурье. Непрерывное и дискретное преобразования Фурье.

Алгебраические структуры: группы, кольца, поля. Конечные кольца и поля, их применение в криптографии.

Раздел 3. Основы криптографии

Симметричные и асимметричные алгоритмы шифрования, их применение в системах передачи и хранения информации. Блочные ШИФРЫ, режимы их функционирования. Основные атаки на блочные шифры. Поточковые шифры, Шифр Вернама. Криптостойкие генераторы псевдослучайных чисел. Теоретическая стойкость шифров. Совершенные и идеальные шифры.

Методы получения случайных последовательностей, их использование в криптографии. Криптографические хеш-функции. Их свойства и использование в криптографии. Методы получения псевдослучайных последовательностей, их использование в криптографии.

Криптографические протоколы распределения ключей. Криптографические протоколы идентификации. Методы цифровой (электронной) подписи. Стойкость систем с открытыми ключами. Криптографические средства, используемые при построении платежных систем. Электронные деньги. Алгоритмические основы криптографии с открытыми ключами. Методы выполнения основных криптографических операций.

Статистическое тестирование случайных и псевдослучайных последовательностей в криптографии. Использование статистических тестов при анализе криптосистем.

Российские стандарты на криптографические алгоритмы. История криптографии и ее основные достижения.

3.3 Перечень вопросов для вступительного испытания.

Вопросы по специальной дисциплине:

Раздел 1. Организационные основы информационной безопасности

1. Основные понятия и принципы теории информационной безопасности.
2. Угрозы информационной безопасности, их анализ.
3. Виды информации, методы и средства обеспечения информационной безопасности.
4. Методы нарушения конфиденциальности, целостности и доступности информации.
5. Основы комплексного обеспечения информационной безопасности.
6. Модели, стратегии и системы обеспечения информационной безопасности.
7. Лицензирование и сертификация в области защиты информации.
8. Правовые основы защиты информации с использованием технических средств.
9. Защита интеллектуальной собственности.
10. Основы законодательства в области защиты информации.

Раздел 2. Избранные разделы математики

1. Матрицы. Виды матриц. Линейные операции над матрицами. Произведение матриц. Элементарные преобразования матриц. Обратная матрица и ее вычисление.
2. Бесконечная числовая последовательность и ее предел. Неопределенности. Замечательные пределы. Непрерывность функции. Классификация разрывов.
3. Дифференцирование функции одной переменной. Основные теоремы дифференциального исчисления. Производные элементарных функций. Правило Лопиталя раскрытия неопределенностей. Исследование функции одной переменной.
4. Неопределенный интеграл, Определение и существование. Свойства. Приемы интегрирования.
5. Определенный интеграл Римана. Несобственные интегралы,
6. Числовые ряды. Признаки сходимости. Знакопеременные ряды. Абсолютная и условная сходимость. Степенные ряды. Радиус сходимости. Ряд Тейлора. Разложение основных функций в степенной ряд.
7. Алгебраические структуры: группы, кольца, поля. Конечные кольца и поля, их применение в кодировании и криптографии.
8. Случайные события и случайные величины. Зависимость и независимость. Теоремы сложения и умножения вероятностей. Основные законы распределения случайных величин. Математическое ожидание и дисперсия.
9. Марковские процессы и цепи. Понятия стационарности и эргодичности случайного процесса. Классификация марковских цепей и их состояний. Уравнения Колмогорова для переходных вероятностей марковского процесса. Предельные вероятности.
10. Случайный процесс. Понятие процесса с независимыми приращениями. Теорема о свойствах его конечномерных распределений. Основные модели процессов с независимыми приращениями: пуассоновский, сложный пуассоновский и винеровский процессы.
11. Теория систем массового обслуживания. Система массового обслуживания без очереди и с очередью.
12. Интерполяция функции. Интерполяция многочленами.
13. Комбинаторные задачи и основные принципы комбинаторики. Перестановки и подстановки. Размещения и сочетания без повторений. Размещения и сочетания с повторениями.

Раздел 3. Основы криптографии

1. Криптография. Основные термины и определения. Классификация шифров.
2. Шифры замены. Классификация и основные методы шифрования.
3. Шифры перестановки. Классификация и основные методы шифрования.
4. Шифры гаммирования. Классификация и основные методы шифрования.
5. Способы генерации истинно случайных и псевдослучайных гамм.
6. Комбинированные блочные шифры. Режимы шифрования.
7. Шифрование с открытым ключом.
8. Криптографические хэш-функции.
9. Криптографические протоколы. Основные понятия.
10. Протоколы обмена ключами.
11. Протоколы аутентификации. Разновидности и краткая характеристика.
12. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
13. Протоколы контроля целостности. Разновидности и краткая характеристика.
12. Криптография в электронных платежах. Разновидности и краткая характеристика.
13. Электронное голосование. Разновидности и краткая характеристика.
14. Протоколы разбиения и разделения секрета.
15. Тайные многосторонние вычисления.
16. Основы теории чисел. Простые числа. Разложение числа на простые сомножители. Тестирование числа на простоту.
17. Основные сведения о криптоанализе и атаки на криптосистемы.
18. Российские стандарты на криптографические алгоритмы.

3.4. Критерии оценивания результата вступительного испытания

Уровень знаний поступающего оценивается экзаменационной комиссией по балльной системе.

Таблица - Критерии экспертного анализа и оценки качества знаний на вступительном экзамене по специальной дисциплине за вопросы на билет

Критерий	Количество баллов
В ответе отражены основные концепции и теории по данному вопросу, проведен их критический анализ и сопоставление, описанные теоретические положения иллюстрируются практическими примерами и экспериментальными данными. Абитуриентом формулируется и обосновывается собственная точка зрения на заявленные проблемы, материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов	100 - 80
В ответе описываются и сравниваются основные современные концепции и теории по данному вопросу, описанные теоретические положения иллюстрируются практическими примерами, абитуриентом формулируется собственная точка зрения на заявленные проблемы, однако он испытывает затруднения в ее аргументации. Материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов	79 - 59
В ответе отражены лишь некоторые современные концепции и теории по данному вопросу, анализ и сопоставление этих теорий не проводится. Абитуриент испытывает значительные затруднения при иллюстрации теоретических положений практическими примерами. У абитуриента отсутствует собственная точка зрения	58 - 45

на заявленные проблемы. Материал излагается профессиональным языком с использованием соответствующей системы понятий и терминов.	
Ответ не отражает современные концепции и теории по данному вопросу. Абитуриент не может привести практических примеров. Материал излагается языком, без использования терминологий и понятий соответствующей научной области.	44 - 0

Максимальное количество баллов, полученных за ответы на 3 вопроса, составляет 100 баллов. Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания, составляет 45 баллов.

4. СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

4.1. Основная литература

Раздел 1

1. Бубнов, А.А. Основы информационной безопасности: Учебное пособие / А.А. Бубнов. - М.: Academia, 2018. - 480 с.
2. Башлы, П. Н. Информационная безопасность: учебно-практическое пособие : учебное пособие / П. Н. Башлы, Е. К. Баранова, А. В. Бабаш. – Москва : Евразийский открытый институт, 2011. – 375 с
3. Методы и средства инженерно-технической защиты информации : учебное пособие / В.И. Аверченков [и др.]. — Брянск : Брянский государственный технический университет, 2012. — 187 с. — ISBN 5-89838-357-3
4. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие : [16+] / Ю. Н. Рагозин. – Санкт-Петербург : Интермедия, 2018. – 168 с. : схем., табл.

Раздел 2

1. Шипачев, В.С. Высшая математика : Учебник / Московский государственный университет им. М.В. Ломоносова, факультет вычислительной математики и кибернетики. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2018. - 479 с. - ISBN 978-5-16-010072-2
2. Балдин, К.В. Теория вероятностей и математическая статистика [Электронный ресурс] / К. В. Балдин, В. Н. Башлыков, А. В. Рукосуев. - Электрон. текст. дан. - 2-е изд. - Москва : Дашков и К°, 2018. - 472 с.
3. Письменный, Д. Т. Конспект лекций по теории вероятностей, математической статистике и случайным процессам : курс лекций/ Д. Т. Письменный. - 5-е изд. - М.: Айрис-пресс, 2010. - 287с.
4. Кочетков, Е.С. Теория вероятностей и математическая статистика : Учебник / Московский авиационный институт (национальный исследовательский университет). - 2, испр. и перераб. - Москва : Издательство "ФОРУМ", 2018. - 240 с.

Раздел 3

1. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: Учебное пособие для вузов. Изд. 2-е стереотипное. М.: Горячая линия-Телеком, 2012. 229 с.
2. Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие : [16+] / Н. Г. Бутакова, Н. В. Федоров. – Санкт-Петербург : Интермедия, 2020. – 380 с

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва : Издательство Юрайт, 2019. — 349 с..

4. Кукина Е.Г. Введение в криптографию [Электронный ресурс]: сборник задач и упражнений/ Кукина Е.Г., Романьков В.А.— Электрон. текстовые данные.— Омск: Омский государственный университет, 2013.— 91 с. - Режим доступа: <http://www.iprbookshop.ru/24876>.— ЭБС «IPRbooks», по паролю.

4. 2. Дополнительная литература

1) Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2) Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3) Федеральный Закон от 07 июля 2003 г. № 126-ФЗ «О связи».

4) ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

5) "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

4.3 Информационно–справочные системы

1. Российская государственная библиотека - <http://www.rsl.ru/>

2. Государственная публичная научно-техническая библиотека России - <http://www.gpntb.ru/>