

УТВЕРЖДАЮ

Проректор по науке

А.В. Германенко

« 2022 г.



ПРОГРАММА

вступительных испытаний в аспирантуру

по научной специальности

2.3.6 «Методы и системы защиты информации, информационная без-
опасность»

Екатеринбург

2022

Содержание

1.	Назначение и область применения.....	3
2.	Содержание программы	4
	2.3.6 Методы и системы защиты информации, информационная безопасность.....	4
3.	Примеры вопросов для вступительного испытания.....	9
	2.3.6 Методы и системы защиты информации, информационная безопасность.....	9
4.	Критерии оценки знаний претендентов на поступление в аспирантуру на научную специальность 2.3.6 «Методы и системы защиты информации, информационная безопас- ность»	14
5.	Список рекомендуемой литературы (основная и дополнительная).....	15
	2.3.6 Методы и системы защиты информации, информационная безопасность.....	15
6.	Рекомендуемые Интернет-ресурсы	20
7.	Лист согласования.....	23

1. Назначение и область применения

Программа определяет требования к содержанию вступительных испытаний в аспирантуру по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Предназначена для подготовки к вступительному экзамену в аспирантуру по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Целью вступительного экзамена является проверка способности и готовности претендента к обучению по программам подготовки научных и научно-педагогических кадров в аспирантуре в соответствии с федеральными государственными требованиями (приказ министерства науки высшего образования от 20.10.2021 г. № 951), выполнению профессиональных задач в сфере научной деятельности.

Форма проведения вступительного испытания

Вступительные испытания по специальной дисциплине в аспирантуру проводятся в форме устного собеседования по вопросам, перечень которых доводится до сведения поступающих путем опубликования программы вступительных испытаний на официальном сайте университета.

Требования к процедуре вступительного экзамена

Требования к порядку планирования, организации и проведения вступительного экзамена, к структуре и форме документов по его организации определены Правилами приема поступающих на обучение по программам подготовки научных и научно-педагогических кадров в аспирантуре.

Содержание программы базируется на следующих дисциплинах: математика; математический анализ, линейная алгебра, численные методы, информатика, финансовый анализ, вычислительная математика; математическое моделирование; программирование на языках высокого уровня; объектно-ориентированное программирование; базы данных; структуры и алгоритмы обработки данных; финансовый анализ, организация и функционирование ЭВМ; сети ЭВМ и телекоммуникации; теория систем и системный анализ; теория автоматического управления; компьютерная графика; автоматизация конструкторского и технологического проектирования, разработка систем автоматизированного проектирования.

2. Содержание программы

Настоящая программа охватывает основополагающие разделы наук и технологий в рамках научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность». Так же содержит список рекомендуемой литературы, рекомендуемые Интернет-ресурсы.

2.3.6 Методы и системы защиты информации, информационная безопасность

Математика

Дифференциальное исчисление. Основные теоремы дифференциального исчисления: теорема Ролля, Лагранжа и Коши о конечных приращениях; локальная формула Тейлора; асимптотические разложения элементарных функций; формула Тейлора с остаточным членом; применение дифференциального исчисления к исследованию функций, признаки постоянства, монотонность, экстремумы, выпуклость, точки перегиба, раскрытие неопределенностей, геометрические приложения.

Интегральное исчисление. Определенный интеграл Римана по отрезку. Существование интеграла. Интегрируемость непрерывной функции; интегрируемость ограниченной функции с конечным числом точек разрыва. Интегрируемость монотонной функции. Теоремы о среднем значении интеграла. Замена переменного в определенном интеграле. Формула интегрирования по частям. Формула Ньютона-Лейбница.

Дифференцируемость функций нескольких переменных. Частные производные. Полный дифференциал. Достаточное условие дифференцируемости. Достаточное условие равенства смешанных производных. Формула Тейлора. Локальный экстремум; необходимое и достаточное условия локального экстремума. Теоремы существования, непрерывности, дифференцируемости неявной функции. Условный локальный экстремум; метод неопределенных множителей Лагранжа.

Числовые ряды: сходимость и сумма числового ряда; критерий Коши; признаки сходимости Даламбера, Коши, интегральный признак сходимости, признак Лейбница; абсолютная и условная сходимость. Функциональные последовательности и ряды: равномерная сходимость; признаки равномерной сходимости; теорема о предельном переходе; теорема о непрерывности, почленном интегрировании и дифференцировании; степенные ряды.

Линейные пространства и их подпространства. Базис, размерность. Теорема о ранге матрицы. Системы линейных уравнений. Теорема Кронеккера-Капелли. Билинейные и квадратичные формы в линейных пространствах. Приведение квадратичных форм к нормальному виду. Закон инерции. Линейные отображения в линейных пространствах.

События и их вероятности. Определения вероятности событий: теоретико-множественное, классическое, статистическое, аксиоматика Колмогорова. Условная вероятность. Независимые события. Формулы полной вероятности и Байеса. Схемы независимых испытаний Бернулли, асимптотические формулы для вычисления биномиальных вероятностей (Муавра-Лапласа, Пуассона). Случайные величины. Распределения случайных величин; дискретное распределение, абсолютно непрерывное распределение. Функция распределения и ее свойства. Плотность распределения. Числовые характеристики случайной величины: математическое ожидание, дисперсия, ковариация, коэффициент корреляции и их свойства. Классические распределения: Бернулли, биномиальное, Пуассона, равномерное, нормальное и показательное.

Элементы теории оценивания. Метод максимального правдоподобия. Неравенство Рао-

Крамера. Методы построения доверительных интервалов. Простые и сложные гипотезы. Проверка непараметрических гипотез. Критерии согласия: Колмогорова, Пирсона.

Элементы регрессионного анализа. Линейная модель в регрессионном анализе. Метод наименьших квадратов. Оценка параметров линейной модели. Оценка точности линейных моделей и проверка их адекватности. Определение значимости коэффициентов. Применение метода Монте-Карло при решении статистических задач. Моделирование случайных величин и векторов с заданными законами распределения. Общие методы моделирования случайных процессов.

Математическое моделирование.

Понятия о системном подходе, системном анализе. Выделение системы из среды, определение системы. Системы и закономерности их функционирования и развития. Управляемость, достижимость, устойчивость. Свойства системы: целостность и членимость, связность, структура, организация, интегрированные качества.

Модели систем: статические, динамические, концептуальные, топологические, формализованные (процедуры формализации моделей систем), информационные, логико-лингвистические, семантические, теоретико-множественные и др.

Основные методологические принципы анализа систем. Задачи системного анализа. Роль человека в решении задач системного анализа.

Определение динамических характеристик. Идентификация на основе методов оценивания. Основные методы оценивания параметров. Оценивание по методу наименьших квадратов. Марковские оценки. Оценки по методу максимального правдоподобия. Байесовские оценки. Рекуррентные методы оценивания. Оценивание параметров и состояния объектов. Фильтр Калмана-Бьюси. Одновременное оценивание параметров и состояний. Методы квазилинеаризации и инвариантного погружения.

Вычислительные алгоритмы и экспертные системы

Вычислительные алгоритмы. Понятие алгоритма. Примеры (метод вилки, метод итераций, метод Ньютона). Алгоритмическая погрешность. Типы вычислительных процессов. Итерационные алгоритмы. Алгоритмы при использовании метода Монте-Карло. Методы решения интегро-дифференциальных уравнений - моделей объектов с распределенными параметрами.

Основные разделы теории и приложений искусственного интеллекта. Описание и постановка задачи. Задачи в пространстве состояний, в пространстве целей. Классификация задач по степени сложности. Линейные алгоритмы. Полиномиальные алгоритмы. Экспоненциальные

Вычислительный эксперимент. Принципы проведения вычислительного эксперимента. Исследование операций и задачи искусственного интеллекта. Информационные процедуры. Распознавание образов.

Компьютерные технологии обработки информации

Понятие информационной системы, банки и базы данных. Логическая и физическая организация баз данных. Модели представления данных, архитектура и основные функции СУБД. Распределенные БД. Принципиальные особенности и сравнительные характеристики файл-серверной, клиент-серверной и интранет технологий распределенной обработки данных. Реляционный подход к организации БД.

Сети ЭВМ и телекоммуникации

Основные сетевые концепции. Глобальные, территориальные и локальные сети. Проблемы стандартизации. Сетевая модель OSI. Модели взаимодействия компьютеров в сети. Функции сетевого и транспортного протоколов. Краткая характеристика сетевых протоколов.

Функции сетевых операционных систем. Характеристики и типы каналов передачи данных: радиоканалы, аналоговые каналы, цифровые каналы и т.д. Виды модуляции. Помехоустойчивое кодирование данных. Методы уплотнения каналов. Обзор и сравнительный анализ популярных семейств сетевых ОС.

Блок специализированной подготовки по Информационной безопасности

Понятие системы управления информационной безопасностью. Типовая структура СУИБ. Функции СУИБ. Стандартизация в области обеспечения информационной безопасности. Международные организации по стандартизации. Основные международные и национальные стандарты в области управления информационной безопасностью на основе информационной системы. ГОСТ Р ИСО/МЭК 27001. Область применения, назначение, основные термины. Оценка защищенности продуктов и систем информационных технологий. Стандарт ISO/IEC 15408 – «Общие критерии». Функциональные требования и требования доверия к безопасности. Понятие информационного риска. Методики анализа информационных рисков. Основные характеристики COBRA, CRAMM, Risk Watch, АванГард.

Аттестация объектов информатизации по требованиям безопасности информации: аттестация автоматизированных систем, средств связи, обработки и передачи информации; аттестация помещений; аттестация технических средств, установленных в выделенных помещениях. Классификация и определение технических каналов утечки информации. Защита информации от утечки по техническим каналам. Специальные исследования технических средств на наличие технических каналов утечки информации. Принципы действия сигнализационных датчиков инфракрасного и радиотехнического типов. Построение чувствительных элементов и трактов обработки тревожной информации. Требования к размещению датчиков на объекте. Общая характеристика систем управления физическим и логическим доступом на объект информатизации. Парольные системы. Физические носители ключевой информации. Биометрические системы. Сравнительная характеристика методов идентификации и аутентификации.

Государственная система технического регулирования и стандартизации в Российской Федерации. Основные нормативно-технические документы Российской Федерации в области обеспечения информационной безопасности. Система защиты государственной тайны; правовой режим защиты государственной тайны; правовое регулирование взаимоотношений администрации и персонала в области защиты информации; правовые режимы конфиденциальной информации.

Принцип работы средств терминального доступа. Протоколы SSH, X11, RDP, VNC, SPICE. Межсетевые экраны. Типы межсетевых экранов. Выбор и адаптация межсетевых экранов к практическим задачам. Внутренняя архитектура межсетевых экранов, пакетные фильтры, шлюзы уровня сеанса, посредники прикладного уровня, инспекторы состояний. Принципы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux. Организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации пользователей. Краткая характеристика моделей разграничения доступа: дискреционной, мандатной, ролевой, атрибутивной.

Типы сигналов, их дискретизация и восстановление. Спектральная плотность сигналов. Частота Найквиста, теорема Котельникова. Особенности цифровых систем многоканальных передач сообщений: способы объединения цифровых потоков; особенности передачи дискретных сообщений по цифровым каналам. Спектральный анализ непрерывных непериодических сигналов, дискретных сигналов, дискретных сигналов конечной длительности.

Понятия математических моделей и методов. Типы и виды данных. Понятие временного ряда. Стохастические и детерминированные модели. Задача прогноза и понятие доверительного интервала. Прогнозирование трендов. Понятие перспективной и ретроспективной экстраполяции. Прогнозирование с минимальной среднеквадратичной ошибкой и их свойства.

Большие данные (big data). Характерные черты больших данных. Программные средства обработки больших данных. Модель MapReduce. Построение линейной регрессии по выборочным данным. Расчёт выборочного коэффициента корреляции. Понятие машинного обучения. Этапы обучения и построения модели. Типы задач, решаемых с помощью машинного обучения. Понятие нейронной сети. Задача поиска ассоциативных правил. Алгоритмы Apriori и FPGrowth. Задачи классификации. Построение решающих деревьев. Байесовская классификация. Метрические методы классификации. Задачи кластеризации. Метод k средних. Задачи поиска аномалий (outlier detection).

Циклические коды. Коды, исправляющие пакеты ошибок, граница Рейджера, алгоритм исправления пакетов ошибок. Основные параметры кодов, исправляющих ошибки: длина, скорость, минимальное расстояние. Связь между минимальным расстоянием и корректируемыми возможностями кода. Граница Хэмминга. Определение поточного шифра. Требования к стойкости поточного шифра. Конструкции поточных шифров. Синхронные и самосинхронизирующиеся поточные шифры. Групповые шифры гаммирования, шифры модульного гаммирования. Абсолютный стойкий шифр Вернама. Примеры. Генераторы случайных и псевдослучайных чисел. Основные принципы построения. Равномерно распределенные случайные последовательности, псевдослучайные последовательности. Требования к управляющей гамме генератора псевдослучайных чисел. Симметричные блочные шифры. Принципы построения подстановки итеративного симметричного блочного шифра. Конструкции блочных шифров: шифры, основанные на схеме Фейстеля, SP-сети. Примеры. Открытое распределение ключей. Протокол Диффи-Хеллмана. Схемы открытого шифрования на основе однонаправленной функции с потайной дверью (схемы RSA, Рабина и др.). Схемы открытого шифрования на основе дискретного логарифмирования (схема Эль-Гамала и др.). Определение схемы электронной подписи. Стойкость схем электронной подписи. Сравнительная оценка симметричных и асимметричных методов аутентификации сообщений. Нормативное правовое и нормативно-техническое регулирование использования электронной подписи для обеспечения безопасности электронного документооборота в РФ, создания удостоверяющих центров. Закон РФ «Об электронной подписи». Спецификация SSL/TLS. Назначение, область применения, аутентификация и шифрование данных. Спецификация IPSec. Назначение, область применения, аутентификация и шифрование данных. Нормативные документы в области применения средств криптографической защиты информации. Стандартизация, лицензирование и сертификация в области проектирования средств защиты информации. Использование криптографических средств для обеспечения безопасности персональных данных.

Оценивание защищенности компьютерной системы по анализу реализованности установленных требований. Количественные параметры (метрики) защищенности компьютерной системы при охватно-номинальном подходе. Аудит информационной безопасности организаций. Внешний и внутренний аудит. Стандарты аудита. Методы и инструментальные средства проведения аудита информационной безопасности. Обеспечение информационной безопасности информационных систем. Политика безопасности. Структура документов, разрабатываемых для документирования требований политики безопасности к информационным системам. Событие и инцидент информационной безопасности. Управление инцидентами информаци-

онной безопасности. Кадровое обеспечение информационной безопасности. Методы и средства подбора и расстановки кадров. Особенности взаимодействия служб безопасности с персоналом предприятия. Система обеспечения психологической устойчивости к криминальным воздействиям. Методы психофизиологического тестирования.

Понятие и систематика компьютерных атак. Этапы сетевой атаки. База знаний Mitre Att&ck. Принципы работы систем обнаружения атак. Основные типы СОА. Параметры сетевого трафика, анализируемые СОА. Примеры. Законодательство РФ в области защиты критической информационной инфраструктуры. Ответственность за неправомерное воздействие на КИИ РФ. Особенности компьютерного следообразования в операционных система семейства Windows и Linux. Аудит событий и его безопасность. Основные свойства файловой системы NTFS. Понятие об MFT. Структура записи в MFT. Организация резидентных и нерезидентных файлов в NTFS. Понятие об EFS. Структура зашифрованного файла. Основные свойства файловой системы EXT*FS. Структура метаданных и их размещение на дисковом пространстве. Права доступа. Работа с объектами файловой системы. Преступления в сфере компьютерной информации; экспертиза преступлений в области компьютерной информации; криминалистические аспекты проведения расследований.

Состав технических параметров компьютерного инцидента. Базовые категории и типы событий, по которым инициируется информационное взаимодействие. Предоставление информации в ГосСОПКА. Определение и классификация вредоносных программ для ЭВМ. Деструктивные возможности компьютерных программ. Программные методы вредоносного удаления, копирования, блокирования, модификации компьютерной информации и нарушения работы ЭВМ.

Методы антивирусной защиты. Организационные и программные средства антивирусной защиты. Построение изолированной программной среды.

Реляционные СУБД. Реляционная алгебра. Нормальные формы. Язык манипулирования данными SQL. Первичные и внешние ключи в таблицах реляционной БД. Нереляционные СУБД (технология NoSQL): модель «ключ – значение», документориентированные, графовые СУБД. Запросы к нереляционным СУБД.

3. Примеры вопросов для вступительного испытания

2.3.6 Методы и системы защиты информации, информационная безопасность

Вопросы для вступительных испытаний

Часть 1.

- 1) Дифференциальное исчисление. Основные теоремы дифференциального исчисления
- 2) Применение дифференциального исчисления к исследованию функций, признаки постоянства, монотонность, экстремумы, выпуклость, точки перегиба, геометрические приложения.
- 3) Интегральное исчисление. Определенный интеграл Римана по отрезку. Существование интеграла.
- 4) Интегрируемость непрерывной функции; интегрируемость ограниченной функции с конечным числом точек разрыва. Интегрируемость монотонной функции.
- 5) Теоремы о среднем значении интеграла. Замена переменного в определенном интеграле.
- 6) Формула интегрирования по частям. Формула Ньютона-Лейбница.
- 7) Дифференцируемость функций нескольких переменных. Частные производные. Полный дифференциал.
- 8) Достаточное условие дифференцируемости. Достаточное условие равенства смешанных производных.
- 9) Интегральное исчисление. Интегральные уравнения Фредгольма и Вольтера 2-го рода
- 10) Формула Тейлора. Локальный экстремум; необходимое и достаточное условия локального экстремума.
- 11) Теоремы существования, непрерывности, дифференцируемости неявной функции. Условный локальный экстремум; метод неопределенных множителей Лагранжа.
- 12) Числовые ряды: сходимость и сумма числового ряда; критерий Коши;
- 13) Функциональные последовательности и ряды: равномерная сходимость; признаки равномерной сходимости;
- 14) Степенные ряды.
- 15) Линейные пространства и их подпространства. Базис, размерность.
- 16) Билинейные и квадратичные формы в линейных пространствах. Приведение квадратичных форм к нормальному виду.
- 17) Приведение матрицы линейного оператора к жордановой форме.
- 18) Дифференциальные уравнения первого порядка. Теорема существования и единственности решения задачи Коши.
- 19) Линейные системы. Определитель Вронского. Теорема Лиувилля.
- 20) Линейные дифференциальные уравнения в частных производных второго порядка, их классификация. Задача Дирихле для уравнения Лапласа.
- 21) События и их вероятности. Определения вероятности событий: теоретико-множественное, классическое, статистическое, аксиоматика Колмогорова.
- 22) Формулы полной вероятности и Байеса. Схемы независимых испытаний Бернулли, асимптотические формулы для вычисления биномиальных вероятностей (Муавра-Лапласа, Пуассона).
- 23) Случайные величины. Распределения случайных величин; дискретное распределение, абсолютно непрерывное распределение.
- 24) Функция распределения и ее свойства. Плотность распределения. Классические распределения: Бернулли, биномиальное, Пуассона, равномерное, нормальное и показательное.
- 25) Свойства точечных оценок параметров. Оценки математического ожидания и дисперсии генеральной совокупности по выборке.
- 26) Проверка гипотезы о типе распределения. Метод моментов для оценки параметров распределения. Критерий Пирсона.

- 27) Система случайных величин. Числовые характеристики. Коэффициент корреляции, его свойства. Выборочный коэффициент корреляции.
- 28) Регрессионный анализ. Проверка значимости линейной модели с помощью критерия Фишера. Проверка значимости линейной модели с помощью критерия Стьюдента.
- 29) Маргинальные законы распределения. Начальные и центральные моменты. Гауссовское распределение (одномерное и многомерное) и распределения, связанные с ним.
- 30) Функции от случайных величин. Виды сходимости последовательности случайных величин.
- 31) Закон больших чисел; теоремы Чебышева и Бернулли. Центральная предельная теорема. Коэффициент корреляции. Понятие случайного процесса. Классификация случайных процессов.
- 32) Стационарные случайные процессы. Гауссовский стационарный процесс.
- 33) Эргодические процессы. Корреляционная теория. Спектральное разложение стационарных процессов.
- 34) Цепи Маркова. Марковские процессы. Непрерывный марковский процесс.
- 35) Уравнение Колмогорова. Решение уравнения Колмогорова для простейших случаев.
- 36) Основные задачи, решаемые ЛВС. Модель OSI. Физический и канальный уровни организации ЛВС.
- 37) Физическая и логическая топологии сети. Различные способы доступа к среде передачи. Основные устройства, работающие на этих уровнях.
- 38) Типы вычислительных сетей.
- 39) Методы доступа в локальных вычислительных сетях.
- 40) Высокоскоростные корпоративные, локальные и глобальные сети.
- 41) Характеристики и типы каналов передачи данных.
- 42) Виды модуляции.
- 43) Помехоустойчивое кодирование данных.
- 44) Методы уплотнения каналов.
- 45) Функции сетевого и транспортного протоколов.
- 46) Краткая характеристика сетевых протоколов.
- 47) Распределенные БД. Принципиальные особенности и сравнительные характеристики файл-серверной, клиент-серверной и интернет технологий распределенной обработки данных.

Часть 2.

- 1) Понятие системы управления информационной безопасностью. Типовая структура СУИБ. Функции СУИБ. Стандартизация в области обеспечения информационной безопасности. Международные организации по стандартизации.
- 2) Основные международные и национальные стандарты в области управления информационной безопасностью на основе информационной системы. ГОСТ Р ИСО/МЭК 27001. Область применения, назначение, основные термины.
- 3) Оценка защищенности продуктов и систем информационных технологий. Стандарт ISO/IEC 15408 – «Общие критерии». Функциональные требования и требования доверия к безопасности.
- 4) Понятие информационного риска. Методики анализа информационных рисков. Основные характеристики COBRA, CRAMM, Risk Watch, АванГард.
- 5) Аттестация объектов информатизации по требованиям безопасности информации: аттестация автоматизированных систем, средств связи, обработки и передачи информации; аттестация помещений; аттестация технических средств, установленных в выделенных помещениях.
- 6) Классификация и определение технических каналов утечки информации. Защита информации от утечки по техническим каналам. Специальные исследования технических средств на наличие технических каналов утечки информации.
- 7) Принципы действия сигнализационных датчиков инфракрасного и радиотехнического типов. Построение чувствительных элементов и трактов обработки тревожной информации. Требования к размещению датчиков на объекте.

8) Общая характеристика систем управления физическим и логическим доступом на объект информатизации. Парольные системы. Физические носители ключевой информации. Биометрические системы. Сравнительная характеристика методов идентификации и аутентификации.

9) Государственная система технического регулирования и стандартизации в Российской Федерации. Основные нормативно-технические документы Российской Федерации в области обеспечения информационной безопасности.

10) Система защиты государственной тайны; правовой режим защиты государственной тайны; правовое регулирование взаимоотношений администрации и персонала в области защиты информации; правовые режимы конфиденциальной информации.

11) Принцип работы средств терминального доступа. Протоколы SSH, X11, RDP, VNC, SPICE.

12) Межсетевые экраны. Типы межсетевых экранов. Выбор и адаптация межсетевых экранов к практическим задачам. Внутренняя архитектура межсетевых экранов, пакетные фильтры, шлюзы уровня сеанса, посредники прикладного уровня, инспекторы состояний.

13) Принципы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux.

14) Организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации пользователей. Краткая характеристика моделей разграничения доступа: дискреционной, мандатной, ролевой, атрибутной.

15) Типы сигналов, их дискретизация и восстановление. Спектральная плотность сигналов. Частота Найквиста, теорема Котельникова.

16) Особенности цифровых систем многоканальных передач сообщений: способы объединения цифровых потоков; особенности передачи дискретных сообщений по цифровым каналам.

17) Спектральный анализ непрерывных непериодических сигналов, дискретных сигналов, дискретных сигналов конечной длительности.

18) Понятия математических моделей и методов. Типы и виды данных. Понятие временного ряда. Стохастические и детерминированные модели.

19) Задача прогноза и понятие доверительного интервала. Прогнозирование трендов. Понятие перспективной и ретроспективной экстраполяции. Прогнозирование с минимальной среднеквадратичной ошибкой и их свойства.

20) Большие данные (big data). Характерные черты больших данных. Программные средства обработки больших данных. Модель MapReduce.

21) Построение линейной регрессии по выборочным данным. Расчёт выборочного коэффициента корреляции.

22) Понятие машинного обучения. Этапы обучения и построения модели. Типы задач, решаемых с помощью машинного обучения. Понятие нейронной сети.

23) Задача поиска ассоциативных правил. Алгоритмы Apriori и FPGrowth.

24) Задачи классификации. Построение решающих деревьев. Байесовская классификация. Метрические методы классификации.

25) Задачи кластеризации. Метод k средних.

26) Задачи поиска аномалий (outlier detection).

27) Циклические коды. Коды, исправляющие пакеты ошибок, граница Рейджера, алгоритм исправления пакетов ошибок.

28) Основные параметры кодов, исправляющих ошибки: длина, скорость, минимальное расстояние. Связь между минимальным расстоянием и корректирующими возможностями кода. Граница Хэмминга.

29) Определение поточного шифра. Требования к стойкости поточного шифра. Конструкции поточных шифров. Синхронные и самосинхронизирующиеся поточные шифры. Групповые шифры гаммирования, шифры модульного гаммирования. Абсолютный стойкий шифр Вернама. Примеры.

30) Генераторы случайных и псевдослучайных чисел. Основные принципы построения. Равномерно распределенные случайные последовательности, псевдослучайные последовательности. Требования к управляющей гамме генератора псевдослучайных чисел.

31) Симметричные блочные шифры. Принципы построения подстановки итеративного симметричного блочного шифра. Конструкции блочных шифров: шифры, основанные на схеме Фейстеля, SP-сети. Примеры.

32) Открытое распределение ключей. Протокол Диффи-Хеллмана.

33) Схемы открытого шифрования на основе однонаправленной функции с потайной дверью (схемы RSA, Рабина и др.).

34) Схемы открытого шифрования на основе дискретного логарифмирования (схема Эль-Гамала и др.).

35) Определение схемы электронной подписи. Стойкость схем электронной подписи. Сравнительная оценка симметричных и асимметричных методов аутентификации сообщений.

36) Нормативное правовое и нормативно-техническое регулирование использования электронной подписи для обеспечения безопасности электронного документооборота в РФ, создания удостоверяющих центров. Закон РФ «Об электронной подписи».

37) Спецификация SSL/TLS. Назначение, область применения, аутентификация и шифрование данных.

38) Спецификация IPsec. Назначение, область применения, аутентификация и шифрование данных.

39) Нормативные документы в области применения средств криптографической защиты информации. Стандартизация, лицензирование и сертификация в области проектирования средств защиты информации. Использование криптографических средств для обеспечения безопасности персональных данных.

40) Оценивание защищенности компьютерной системы по анализу реализованности установленных требований. Количественные параметры (метрики) защищенности компьютерной системы при охватно-номинальном подходе.

41) Аудит информационной безопасности организаций. Внешний и внутренний аудит. Стандарты аудита. Методы и инструментальные средства проведения аудита информационной безопасности.

42) Обеспечение информационной безопасности информационных систем. Политика безопасности. Структура документов, разрабатываемых для документирования требований политики безопасности к информационным системам. Событие и инцидент информационной безопасности. Управление инцидентами информационной безопасности.

43) Кадровое обеспечение информационной безопасности. Методы и средства подбора и расстановки кадров. Особенности взаимодействия служб безопасности с персоналом предприятия. Система обеспечения психологической устойчивости к криминальным воздействиям. Методы психофизиологического тестирования.

44) Понятие и систематика компьютерных атак. Этапы сетевой атаки. База знаний Mitre Att&ck.

45) Принципы работы систем обнаружения атак. Основные типы СОА. Параметры сетевого трафика, анализируемые СОА. Примеры.

46) Законодательство РФ в области защиты критической информационной инфраструктуры. Ответственность за неправомерное воздействие на КИИ РФ.

47) Особенности компьютерного следообразования в операционных системах семейства Windows и Linux. Аудит событий и его безопасность.

48) Основные свойства файловой системы NTFS. Понятие об MFT. Структура записи в MFT. Организация резидентных и нерезидентных файлов в NTFS. Понятие об EFS. Структура зашифрованного файла.

49) Основные свойства файловой системы EXT*FS. Структура метаданных и их размещение на дисковом пространстве. Права доступа. Работа с объектами файловой системы.

50) Преступления в сфере компьютерной информации; экспертиза преступлений в области компьютерной информации; криминалистические аспекты проведения расследований.

51) Состав технических параметров компьютерного инцидента. Базовые категории и типы событий, по которым инициируется информационное взаимодействие. Предоставление информации в ГосСОПКА.

52) Определение и классификация вредоносных программ для ЭВМ. Деструктивные возможности компьютерных программ. Программные методы вредоносного удаления, копирования, блокирования, модификации компьютерной информации и нарушения работы ЭВМ.

53) Методы антивирусной защиты. Организационные и программные средства антивирусной защиты. Построение изолированной программной среды.

54) Реляционные СУБД. Реляционная алгебра. Нормальные формы. Язык манипулирования данными SQL. Первичные и внешние ключи в таблицах реляционной БД.

55) Нереляционные СУБД (технология NoSQL): модель «ключ – значение», документориентированные, графовые СУБД. Запросы к нереляционным СУБД.

4. Критерии оценки знаний претендентов на поступление в аспирантуру на научную специальность 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Оценка ответов претендентов на поступление в аспирантуру по данной научной специальности производится по 100 балльной шкале и выставляется согласно критериям, приведенным в таблице.

Критерии оценки ответов претендентов при поступлении в аспирантуру

Оценка	Критерии
80–100 баллов	<ol style="list-style-type: none"> 1. Ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. 2. Демонстрируются глубокие знания по дисциплине. 3. Делаются обоснованные выводы. 4. Ответ самостоятельный, при ответе использованы знания, приобретённые ранее.
60–79 баллов	<ol style="list-style-type: none"> 1. Ответы на поставленные вопросы излагаются систематизировано и последовательно. 2. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. 3. Материал излагается уверенно, в основном правильно даны все определения и понятия. 4. Допущены небольшие неточности при выводах и использовании терминов.
30–59 баллов	<ol style="list-style-type: none"> 1. Допускаются нарушения в последовательности изложения при ответе. 2. Демонстрируются поверхностные знания дисциплины. 3. Имеются затруднения с выводами. 4. Определения и понятия даны не чётко.
0–29 баллов	<ol style="list-style-type: none"> 1. Материал излагается непоследовательно, сбивчиво, не представляет определённой системы знаний по дисциплине. 2. Не даны ответы на дополнительные вопросы комиссии. 3. Допущены грубые ошибки в определениях и понятиях.

5. Список рекомендуемой литературы (основная и дополнительная)

2.3.6 Методы и системы защиты информации, информационная безопасность

Основная литература

- 1) Вострецова Е.В., Основы информационной безопасности, Екатеринбург, Издательство Уральского университета, 2019, 204 с.
- 2) Поршневу С.В. Компьютерное моделирование физических процессов в пакете MATLAB, Горячая линия- Телеком, 2020. 808 с.
- 3) Гибилинду Р.В., Коллеров А.С., Синадский Н.И., Хорьков Д.А., Фартушный А.В. Аудит информационной безопасности компьютерных систем, Учебное пособие для вузов, Горячая линия- Телеком, 2021 г., 126 стр.
- 4) Коллеров А.С., Синадский Н.И., Хорьков Д.А., Системы обнаружения компьютерных атак, Учебное пособие для вузов, Горячая линия- Телеком, 2021 г., 124 стр.
- 5) Литвиненку Н.А., Программирование на C# для платформы .NET Core 3, Курс лекций, Горячая линия- Телеком, 2020 г. 328 стр.
- 6) Литвиненку Н.А., Программирование на C++, Курс лекций, Учебное издание, Горячая линия- Телеком, 2019 г., 310 стр.
- 7) Алексееву А. А. Идентификация и диагностика систем / А. А. Алексееву, Ю. А. Кораблеву, М. Ю. Шестопалову. М.: Академия, 2009. 351 с.
- 8) Арестов В.В., Глазырина П.Ю. Дифференциальные свойства функций одного действительного переменного. Екатеринбург: Изд-во Урал, ун-та, 2013.
- 9) Бройдо, В. Л. Архитектура ЭВМ и систем : учебник / В. Л. Бройдо, О. П. Ильина. - 2-е изд. - СПб. : Питер, 2009. - 720 с. - ISBN 978-5-388-00384-3.
- 10) Бюджетная система России : Учебник / Под ред. Г.Б. Поляка. М.: ЮНИТИ-ДАНА, 2010.
- 11) Ван Хорн Дж.К. Основы управления финансами. / Пер. с англ, под ред. Соколова Я.В. М.: Финансы и статистика, 2009.
- 12) Вентцелю Е. С. Исследование операций. Задачи, принципы, методология / Е.С. Вентцелю. М.: Дрофа, 2010. 208 с.
- 13) Волкова В.Н., Денисова А.А.. Теория систем и системный анализ. М.:ЮРАИТ, 2010.
- 14) Зубов В.И. Лекции по теории управления. СПб.: Лань, 2009.
- 15) Ильин В.А. Линейная алгебра и аналитическая геометрия: учебник. 3-е изд. М: Проспект, 2012.
- 16) Калиткин Н. Н. Численные методы. СПб.: БХВ-Петербург, 2011.
- 17) Каплан А.В., Каплан В.Е., Поршневу С.В., Машенку М.В., Овечкина Е.В. Компьютерный анализ и интерпретация эмпирических зависимостей 2010. 336 с.
- 18) Карташов, Л. П. Параметрический и структурный синтез технологических объектов на основе системного подхода и математического моделирования / Л. П. Карташов, Т. М. Зубкова ; Рос. акад. наук, Урал, отд-ние. - Екатеринбург : УрОРАН, 2009. - 227с.
- 19) Кнут Д.Э. Искусство программирования, том 1. Основные алгоритмы, 4-е изд.: Пер. с англ.: Уч. пос. - М.: Издательский дом «Вильямс», 2010. - 720 с.
- 20) Кнут Д.Э. Искусство программирования, том 2. Получисленные алгоритмы, 4-е изд.: Пер. с англ.: Уч. пос. - М.: Издательский дом «Вильямс», 2010. - 832 с.
- 21) Кнут Д.Э. Искусство программирования, том 3. Сортировка и поиск, 4-е изд.: Пер. с англ.: Уч. пос. - М.: Издательский дом «Вильямс», 2010. - 832 с.
- 22) Колокольцов В, Малафееву О. Математическое моделирование многоагентных систем конкуренции и кооперации. Теория игр для всех. Учебники для вузов. Специальная литература. М.: Лань. 2012
- 23) Кремер Н.Ш. «Теория вероятностей и математическая статистика». М.: Логос, 2010.
- 24) Курош А.Г. Курс высшей алгебры. СПб.: Лань, 2013-432с.
- 25) Мазалов В.В. Математическая теория игр и приложения, Санкт-Петербург, Лань, 2010.

- 26) Мазалов В.В. Математическая теория игр и приложения, Санкт-Петербург, Лань, 2010.
- 27) Мышкис А.Д. Элементы теории математических моделей. УРСС, 2011.
- 28) Норенков И. П. Автоматизированные информационные системы : учеб, пособие для вузов / Норенков И. П. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2011. - 342 с. : ил. - (Информатика в техническом университете). - Библиогр.: с. 342. - ISBN 978-5-7038-3446-6
- 29) Норенков И.П. Основы автоматизированного проектирования : Учебник для вузов / Норенков И. П. - 4-е изд., перераб. и доп. - М. : Изд-во МГТУ им. Н. Э. Баумана, 2009. - 430 с. : ил. - (Информатика в техническом университете). - Библиогр.: с. 426. - ISBN 978-5-7038- 3275-2
- 30) Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб, пособие для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : Питер, 2010. - 943с.
- 31) Певзнер Л. Д. Математические основы теории систем / Л. Д. Певзнер, Е. П. Чураков. М.: Высшая школа, 2009. 503 с.
- 32) Пименов В.Г. Численные методы. Часть 1. Екатеринбург: Изд-во Урал. Ун-та, 2013
- 33) Понтрягин Л.С. Обыкновенные дифференциальные уравнения. М.: URSS, 2011
- 34) Поршнева С.В. Компьютерное моделирование физических процессов в пакете MATLAB, 2020. 900 с.
- 35) Ретгиева А.Н. Оптимальность в динамических и вероятностных моделях. Учебное пособие. Петрозаводск: изд-во ПетрГУ, 2011.
- 36) Симонович С. В. Информатика. Базовый курс / С.В. Симонович и др. - С.-Петербург: Питер, 2009. - 640 с.
- 37) Спиринов Н.А. Математическое моделирование металлургических процессов в АСУ ТП / Н.А. Спиринов, В.В. Лавров, В.Ю. Рыболовлев, Л.Ю. Гилева, А.В. Краснобаев, В.С. Швыдкий, О.П. Онорин, К.А. Щипанов, А.А. Бурыкин; под ред. Н.А.Спирина. - Екатеринбург: ФГАОУ ВПО УрФУ, 2014.-462 с
- 38) Спиринов И.А. Модельные системы поддержки принятия решений в АСУ ТП доменной плавки / Н.А. Спиринов, В.В. Лавров, В.Ю. Рыболовлев и др. - Екатеринбург: ФГАОУ ВПО УрФУ, 2011.-462 с.
- 39) Страхование: учебник/ под ред. Л.А. Орланюк-Малицкой, С.Ю. Яновой.- М.: Издательство Юрайт; ИД Юрайт, 2011.-828с.
- 40) Финансовые рынки и институты. Учебник. Чернухина И.А., Осиповская А.В. М.: Экономика, 2011.
- 41) Харари Ф. Теория графов. М: ЛИБРОКОМ, 2009.
- 42) Шкляр, М. Ф. Основы научных исследований: учебное пособие /М.Ф. Шкляр. - 2- изд. - М.:Изд. «Дашков и К», 2009. - 244 с.
- 43) Шуляк П.Н. Финансы предприятия: Учебник. М.: Дашков и К, 2009
- 44) Национальная система раннего предупреждения о компьютерном нападении: научная монография / Петренко С. А., Ступин Д. Д. / под общей редакцией С. Ф. Боева. Университет Иннополис. – Иннополис: «Издательский Дом «Афина», 2017. – 440 с.
- 45) ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ. системы обнаружения компьютерных атак : учебное пособие / Ф.И. Иванов, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков. — Иркутск: ИГУ, 2012. — 115 с.
- 46) Базы данных. Практическое применение СУБД SQL- и NoSQL-типа для применения проектирования информационных систем : учебное пособие / М.В. Хапченко, В.Л. Симонов, С.А. Мартишин. — Москва: Форум, 2018. — 368 с.
- 47) Курило А.П. Основы управления информационной безопасностью : учебное пособие для вузов. — 2-е изд., испр. / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — М. : Горячая линия-Телеком, 2014. — 244 с.: ил. — (Вопросы управления информационной безопасностью. Выпуск 1).
- 48) Милославская Н.Г. Управление рисками информационной безопасности : учебное пособие для вузов. — 2-е изд., испр. / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — М. : Горячая линия-Телеком, 2014. — 130 с.: ил. — (Вопросы управления информационной безопасностью. Выпуск 2).

Дополнительная литература

- 1) Бен-Ари, М. Языки программирования. Практический сравнительный анализ = Understanding Programming Languages : учебник: пер. с англ / М. Бен-Ари. - М. : Мир, 2000. - 366 с. - ISBN 5-03-003314-9.
- 2) Блинова, Т. А. Компьютерная графика / Т. А. Блинова, В. Н. Порев. - СПб.: ЮНИОР, 2006. - 520 с. - ISBN 966-7323-48-X
- 3) Бобровский, С. И. Delphi 7 : учебный курс / С. И. Бобровский. - СПб. : Питер, 2008. - 736 с. - ISBN 978-5-8046-0086-1.
- 4) Бусленко Н.П. Моделирование сложных систем. -М.: Наука, 1978.-399 с.
- 5) Буч, Г. Язык UML. Руководство пользователя = The Unified Modeling Language User Guide : пер. с англ. Г. Буч, Д. Рамбо, А. Джекобсон. - М. : ДМК Пресс, 2003. - 432 с. : ил. - (Для программистов). - Парал. тит. л. англ.
- 6) Введение в математическое моделирование: Учебное пособие для вузов / В.Н. Ашихмин, М.Г. Бояршинов, М.Б. Гитмай и др. Под ред. П.В.Трусова. - М.: Интернет Инжиниринг, 2000. - 336 с.
- 7) Веллинг, Л. Разработка Web-приложений с помощью PHP и MySQL = PHP and MySQL Web Development [Комплект] / Л. Веллинг, Л. Томсон. - 3-е изд. - М. : Вильямс, 2008. - 880 с. +1 электрон. диск (CD-ROM). - ISBN 978-5-8459-0862-9.
- 8) Веников В.А., Веников Г.В. Теория подобия и моделирования: Учебник, 3-е изд. - М.: Высшая школа, 1984. - 439 с.
- 9) Владимиров В.С. Уравнения математической физики. М.: ФИЗМАТЛИТ, 2008.
- 10) Волков, И. К. Исследование операций: учеб. для вузов; Под ред. В. С. Зарубина, А. П. Крищенко. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. - 436 с.
- 11) Гаврилова, Т. А. Базы знаний интеллектуальных систем : учеб, пособие для вузов / Т. А. Гаврилова, В. Ф. Хорошевский . - СПб. : Питер, 2001. - 384 с. : ил.
- 12) Галисеев, Г. В. Программирование на языке C# : самоучитель / Г. В. Галисеев. - М. : Диалектика, 2006. - 368 с. - ISBN 5-8459-0997-X.
- 13) Гладков, Л. А. Генетические алгоритмы / Л. А. Гладков, В. В. Курейчик, В. М. Курейчик; под ред. В.М. Курейчика. - 2-е изд., испр. и доп. - М.: ФИЗМАТЛИТ, 2006. - 320 с.
- 14) Гридин, В. Н. Мажоритарное уплотнение и кодирование двоичных сигналов: монография / В.Н. Гридин, Р.Б. Мазепа, Б.В. Рощин. - М.: Наука, 2001.-124с.
- 15) Девятков Д.Х. Оптимальное управление нагревом металла в камерных нагревательных печах: монография / Д.Х. Девятков, В.М. Дубинин, В.М. Рябков, М.В. Бушманова, А.Б. Белявский. - Магнитогорск:МГТУ, 2000. - 241 с.
- 16) Джонсон, Г. Разработка клиентских веб-приложений на платформе Microsoft. Net Framework [Комплект] : учебный курс Microsoft / Д. Гленн, Н. Тони . - М. : Русская Редакция ; СПб.: Питер, 2007 - 768 с. + CD-ROM. - ISBN 978-5-91180-833-4.-ISBN 978-5-7502-0316-1.
- 17) Дорфф Р. Современные системы управления. - М.: Мир, 2003. - 543 с.
- 18) Дьячко А.Г. Математическое и имитационное моделирование производственных систем: Научное издание. - М.: МИСИС, 2007. - 540 с.
- 19) Ефимова О.В. Финансовый анализ. Современный инструментарий для принятия управленческих решений. М.: Омега-Л, 2010.
- 20) Жарков, В. А. Компьютерная графика, мультимедиа и игры на Visual C# 2005 / В. А. Жарков. - М.: Жарков Пресс, 2005. - 812 с. - ISBN 5-94212-009-9.
- 21) Капустин, Н. М. Комплексная автоматизация в машиностроении: учебник для вузов/Н. М. Капустин, П. М. Кузнецов, Н. П. Дьяконова; под ред. Н. М. Капустина. - М. : Академия, 2005. - 368 с. - (Высшее профессиональное образование). - Библиогр.: с. 361-362. - ISBN 5-7695-2216-X.
- 22) Карманов, В. Г. Математическое программирование / В. Г. Карманов. - М.: ФИЗМАТЛИТ, 2000. - 264 с.
- 23) Кафаров В.В., Глебов М.Б. Математическое моделирование основных процессов химического производства: Учебное пособие для вузов. - М.: Высшая школа, 1991. - 400с.

- 24) Кафаров В.В., Дорохов И.Н., Липатов Л.Н. Системный анализ процессов химической технологии. - М.: Наука, 1982. - 344 с.
- 25) Колесников А.А. Современная прикладная теория управления / Под ред. А.А.Колесникова. - Таганрог: ТРТУ, 2000, ч. 1 - 400 с.; ч. 2 - 559 с.; ч. 3 - 656 с.
- 26) Краснощеков П.С. Принципы построения моделей / П.С.Краснощеков, А.А.Петров. - М.: МГУ, 1983.-264 с.
- 27) Красовский А.А. Буков В.И., Щедрин В.С. Универсальные алгоритмы оптимального управления непрерывными процессами. - М.: Наука, 1977. - 272 с.
- 28) Лисиенко В.Г., Суханов Е.Л., Морозова В.А., Дмитриев А.Н., Загайнов С.А., Пареньков А.Е. Развитие трехуровневых АСУТП в металлургии (коксовые и бескоксовые процессы): Учебное пособие.- М.: Теплотехник, 2006.-328 с.
- 29) Малый С.А., Андреев Ю.Н. Управление нагревом металла. - М.: Металлургия, 1981. - 272 с.
- 30) Налоговый Кодекс Российской Федерации: части I и II. М.: Ось-89, 2012.
- 31) Никулина Н.Н. Страховой менеджмент: учеб.пособие / Н.Н. Никулина, Н.Д. Эриашвили.- М.: ЮНИТИ-ДАНА, 2011.-703с.
- 32) Новиков, Ф. А. Дискретная математика для программистов: учеб, для вузов / Ф. А. Новиков. - СПб. : Питер, 2001- 304 с. : ил.
- 33) Олифер, В. Г. Сетевые операционные системы: учеб, для вузов / В. Г. Олифер, Н. А. Олифер . - СПб. : Питер, 2001. - 544 с. : ил.
- 34) Онорин О.П. Компьютерные методы моделирования доменного процесса / О.П. Онорин, Н.А. Спириин, В.Л. Терентьев, Л.Ю. Гилева, В.Ю. Рыболовлев, И.Е. Косаченко, В.В. Лавров, А.В. Терентьев. Под ред. Н.А. Спирина. Екатеринбург: УГТУ-УПИ. 2005. 301с.
- 35) Павлов, В. В. Сals-технологии в машиностроении (математические модели): учеб, пособие для вузов /В.В. Павлов. - М.: ИЦ МГТУ СТАНКИН,2002.-328с.
- 36) Петров, М. Н. Компьютерная графика : учеб, пособие для вузов / М. Н. Петров, В. П. Молочков. - 2-е изд. - СПб. : Питер, 2004. - 811 с. - ISBN 5-94723-758-X.
- 37) Растринги Л.А. Современные принципы управления сложными объектами. - М.: Сов. радио, 1980. - 232 с.
- 38) Реклейтис Г., Рейвиндран А., Рэгсдел К. Оптимизация в технике. - М.: Мир, 1986, т.1. 348 с.; т.2. - 320 с.
- 39) Роджерс, Д. Алгоритмические основы машинной графики. - М. : Мир, 1989. - 512 с.
- 40) Роджерс, Д. Математические основы машинной графики. Пер. с англ. / Д. Роджерс, Дж. Адамс. - М.: Мир, 2001. - 604 с. - ISBN 5-03-002143-4.
- 41) Салыга В.И. Идентификация и управление процессами в черной металлургии: учебник для вузов / В.И. Салыга, Н.Н. Карабутов. - М.: Металлургия, 1986. - 192 с.
- 42) Советов Б.Я., Яковлев С. А. Моделирование систем: Учебник для вузов. 3-е издание. М.: Высшая школа, 2004. - 319 с.
- 43) Спириин Н.А. Информационные системы в металлургии: Учебник для вузов / Н.А.Спириин, Ю.В.Ипатов, В.И.Лобанов и др. - Екатеринбург: УГТУ-УПИ, 2001. - 617 с.
- 44) Спириин Н.А. Оптимизация и идентификация технологических процессов в металлургии / Н.А.Спириин, В.В.Лавров, С.И.Паршаков, С.Г.Денисенко. - Екатеринбург, УГТУ-УПИ, 2006. - 307 с.
- 45) Сплетухов Ю.А., Дюжиков Е.Ф. Страхование: Учебное пособие. - 2-е изд., перераб. и доп.-М.: ИНФРА-М, 2010.-357с.
- 46) Тарасик В.П. Математическое моделирование технических систем: Учебник для вузов. М.: Наука, 1997. - 600 с.
- 47) Таха А.Х. Введение в исследование операций: в 2 т. / А.Х. Таха. - М.: Мир, 1985. - 479с.
- 48) Цирлин А.М. Оптимальное управление технологическими процессами: Учебное пособие для вузов. - М.: Энергоатомиздат, 1986. - 400 с.
- 49) Шикин, Е. В. Компьютерная графика. Динамика, реалистичные изображения / Е. В. Шикин, А. В. Боресков. - М.: Диалог-МИФИ, 2005. - 461 с. - ISBN - 5-86404-139-4.

50) Шолохович Ф.А. Лекции по дифференциальным уравнениям. Екатеринбург: Уральское издательство, 2005.

51) Юзвович Л.И. Финансово-кредитный механизм привлечения реальных инвестиций. - Екатеринбург: Изд-во АМБ, 2011.

52) Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков; под ред. Н.И. Синадского. – Екатеринбург: УрФУ, 2012. – 160 с.

53) Мандиа, К. Защита от вторжений. Расследование компьютерных преступлений [Текст] : [пер. с англ.] / К. Мандиа, К. Просис. – М.: ЛОРИ, 2005. – 476 с. : ил. ; 24 см. – Перевод. изд.: Incident response: investigating computer crime / Chris Prosise, Kevin Mandia. – 1500 экз. – ISBN 0-07-213182-9 (в пер.)

54) Лукацкий, А. В. Обнаружение атак [Текст] – 2-е изд., перераб. и доп. / А. В. Лукацкий. – СПб: БХВ-Петербург, 2003. – 608 с. : ил. ; 24 см. – 3000 экз. – ISBN 5-94157-246-8.

55) Gary Hallen, Greg Kellogg Security Monitoring with Cisco Security MARS. – USA: Cisco Press, 2007. – 335 с.

56) Аверченков В.И. Аудит информационной безопасности : учеб. пособие для вузов. — М. : ФЛИНТА, 2011 — 269 с.

57) Аверченков В. И. Аудит информационной безопасности органов исполнительной власти : учеб. пособие / В. И Аверченков, М.Ю. Рытов, А.В. Кувылкин, М.В. Рудановский. — М. : ФЛИНТА, 2011. — 100 с. — Электронный ресурс. Режим доступа : <http://mybrary.ru/users/personal/read/audit-informatsionnoy-bezopasnosti-organov-ispolnitelnoy-vlasti-3-izdanie/>.

58) Астахов А.М. Искусство управления информационными рисками — М. : ДМК Пресс, 2010. — 312 с. — Электронный ресурс. Режим доступа : <http://mybrary.ru/users/personal/read/iskusstvo-upravleniya-informatsio-nnyimi-riskami/>.

59) Галатенко В.А. Стандарты информационной безопасности : учебное пособие. — 2-е издание / под редакцией академика РАН В.Б. Бетелина. — М. : ИНТУИТ.РУ «Интернет-университет Информационных технологий», 2006. — 264 с.

6. Рекомендуемые Интернет-ресурсы

1. <http://www.ascon.ru> - официальный сайт группы компаний «АСКОН»
 2. <http://www.cad.ru> - информационный портал «Все о САПР»
 3. <http://www.catia.ru> - сайт посвящен универсальной CAD/CAM/CAE/PDM-системе CATIA
 4. <http://www.delcam.ru> - официальный сайт компании DelCAM
 5. <http://www.sapr.ru> - электронная версия журнала "САПР и графика", <http://www.cadmaster.ru> - электронная версия журнала "CADmaster",
 6. <http://www.tflex.ru> - официальный сайт компании «Топ Системы» -
 7. Lib.students.ru - Студенческая библиотека lib.students.ru URL: <http://www.lib.students.ru>.
 8. Web-портал компании Microsoft для поддержки программы Access [сайт]. URL: office.microsoft.com/ru-ru/access;
 9. Web-портал компании Microsoft в России [сайт]. URL: www.microsoft.com/ru-ru;
 10. Web-портал компании Oracle в России [сайт]. URL: www.oracle.com/ru;
 11. Web-портал компании SyBase в России [сайт]. URL: www.sybase.ru;
 12. Web-портал по информационным технологиям CIT Forum [сайт]. URL: citforum.ru;
 13. Web-портал по продуктам компании Microsoft [сайт]. URL: msdn.microsoft.com/ru-ru;
 14. Web-ресурс SQL.RU [сайт]. URL: www.sql.ru;
 15. Web-ресурс журнала «Открытые системы» [сайт]. URL: www.osp.ru;
 16. Web-ресурс по информационным технологиям INTERFACE.RU [сайт]. URL: www.interface.ru;
 17. Web-ресурс по СУБД MySQL [сайт]. URL: mysql.ru;
 18. Web-ресурс по СУБД PostgreSQL [сайт]. URL: www.postgresql.org.
 19. Web-ресурс разработчиков информационных систем [сайт]. URL: www.rsdn.ru;
 20. Web-форум SQL.RU [сайт]. URL: www.sql.ru/forum;
 21. Всемирная свободная Интернет-энциклопедия Wikipedia [сайт]. URL: ru.wikipedia.org
 22. Государственная публичная научно-техническая библиотека России URL: <http://www.gpntb.ru/>.
Интернет-портал «Информационно-коммуникационные технологии в образовании» [сайт]. URL: www.ict.edu.ru
- Информационно-поисковая система Google [сайт]. URL: www.google.ru
23. Научная электронная библиотека <http://www.eLIBRARY.ru/>.
 24. Национальный открытый интернет-университет «ИНТУИТ» [сайт]. URL: www.intuit.ru
 25. Официальный сайт Федерального агентства по техническому регулированию и метрологии <http://www.gost.ru/>
 26. Официальный сервер Центрального Банка РФ и Федеральной налоговой службы в интернете: <http://www.cbr.ru>; www.nalog.ru.
 27. Российская Государственная библиотека URL: <http://www.rsl.ru/>.
 28. Российская национальная библиотека URL: <http://www.nlr.ru/>.
 29. Российский портал открытого образования [сайт]. URL: www.openet.edu.ru;
 30. Центр Инноваций компании Microsoft в УрФУ [сайт]. URL: mic.usu.ru;
 31. Электронная библиотека стандартов IT-GOST.RU [сайт]. URL: it-gost.ru
- SANS Institute — Application of Neural Networks to Intrusion Detection — 2001 [Электронный ресурс]. URL: <https://www.sans.org/reading-room/whitepapers/detection/application-neural-networks-intrusion-detection-336> (дата обращения: 17.07.2020).
33. Neural networks in cyber security — 2017 [Электронный ресурс]. URL: <http://www.irjcs.com/volumes/vol4/iss09/08.SISPCS10095.pdf> (дата обращения: 17.07.2020).
 34. Краткий анализ решений в сфере СОВ и разработка нейросетевого детектора аномалий в сетях передачи данных [Электронный ресурс]. URL: <https://habr.com/ru/post/358200/> (дата обращения: 17.07.2020).
 35. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика — 2016 [Электронный ресурс]. URL: http://e-notabene.ru/nb/article_18834.html (дата обращения: 17.07.2020).

36. Application of Neural Networks in Computer Security — 2013 [Электронный ресурс]. URL: <https://www.sciencedirect.com/science/article/pii/S1877705814003579> (дата обращения: 17.07.2020).
61. A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015 — 2016 [Электронный ресурс]. URL: https://www.researchgate.net/publication/309038723_A_review_of_KDD99_dataset_usage_in_intrusion_detection_and_machine_learning_between_2010_and_2015 (дата обращения: 17.07.2020).
37. Neural Networks for Intrusion Detection and Its Applications — 2013 [Электронный ресурс]. URL: <https://pdfs.semanticscholar.org/94f8/e1914ca526f53e9932890a0356394f9806f8.pdf> (дата обращения: 17.07.2020).
38. An incremental growing neural gas learns topologies — 2005 [Электронный ресурс]. URL: https://www.researchgate.net/publication/4202425_An_incremental_growing_neural_gas_learns_topologies (дата обращения: 17.07.2020).
39. Сетевые атаки. Виды. Способы борьбы — 2011 [Электронный ресурс]. URL: <https://moluch.ru/conf/tech/archive/5/1115/> (дата обращения: 17.07.2020).
40. Модифицированный алгоритм растущего нейронного газа, применительно к задаче классификации — 2014 [Электронный ресурс]. URL: <https://cyberleninka.ru/article/v/modifitsirovannyu-algoritm-rastuschego-neyronnogo-gaza-primenitelno-k-zadache-klassifikatsii> (дата обращения: 17.07.2020).
41. Дмитрий Кузнецов. Методология и практика создания SOC. Режим доступа: <https://safe-surf.ru/specialists/article/5197/590047>
42. Сергей Куц. Практический опыт построения корпоративного SOC. Режим доступа: <https://safe-surf.ru/specialists/article/5257/643321>
43. Курило А.П. Аудит информационной безопасности / А.П. Курило, С.Л. Зефиоров, В.Б. Голованов и др. — М. : БДЦ-пресс, 2006.—304 с. — Электронный ресурс. Режим доступа : <http://padaread.com/?book=15183&pg=1>
44. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. — М. : Горячая линия-телеком, 2001г. — 148 с. — Электронный ресурс. Режим доступа : <http://bookre.org/reader?file=550028&pg=1>
45. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. — М. : ДМК Пресс, 2004. — 384 с. — Электронный ресурс. Режим доступа : <http://mybrary.ru/users/personal/read/upravlenie-informatsionnyimi-riskami-ekonomicheski-opravdannaya-bezopasnost/>.

Программу вступительного испытания в аспирантуру по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» разработали:

Профессор, д.т.н., профессор

Профессор, д.т.н., доцент

Доцент, к.т.н., доцент

Зав. кафедрой д.ф.-м.н., профессор



Поршнев С.В.

Духан Е.И

Коллеров А.С.

Волков М.В.



**Уральский
федеральный
университет**

имени первого Президента
России Б.Н.Ельцина

Министерство науки и высшего образования Российской Федерации.
Федеральное государственное автономное образовательное учреждение
высшего образования «Уральский федеральный университет имени первого
Президента России Б.Н.Ельцина» (УрФУ)


Программа вступительных испытаний в аспирантуру

**Научная специальность – 2.3.6 «Методы и системы защиты информа-
ции, информационная безопасность»**

стр. 23 из 23

7. Лист согласования

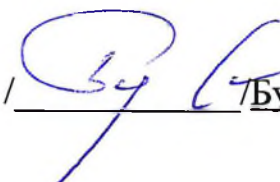
Директор ИРИТ-РТФ

/  /Обабков И.Н./

Директор ИЕНиМ

/  /Рогожин С.А./

Начальник ОПНПК

/  /Бутрина Е.А./