



Минобрнауки России
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Физический факультет

Программа государственного экзамена по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Информационная безопасность автоматизированных систем критически важных объектов»
ФГБОУ ВО «ЧелГУ»

| | | | |
|----------------------|--------|------------------------|---------------|
| Версия документа - 1 | стр. 1 | Первый экземпляр _____ | КОПИЯ № _____ |
|----------------------|--------|------------------------|---------------|

УТВЕРЖДАЮ

Проректор по учебной работе

В.Е. Федоров

« 28 » августа 2020 г.



ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА*

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Информационная безопасность автоматизированных систем критически важных объектов

Присваиваемая квалификация

Специалист по защите информации

Форма обучения

Очная

*Программа государственного экзамена адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2020 г.



Минобрнауки России
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)
Физический факультет

Программа государственного экзамена по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Информационная безопасность автоматизированных систем критически важных объектов»
ФГБОУ ВО «ЧелГУ»

Версия документа - 1

стр. 2

Первый экземпляр _____

КОПИЯ № _____

Программа государственного экзамена принята:

Ученым советом физического факультета

Протокол заседания № 01 от «27» августа 2020 г.

Председатель Ученого совета
физического факультета



Д.А. Захарьевич

Секретарь Ученого совета
физического факультета



М.А. Эбель

Программа государственного экзамена одобрена и рекомендована кафедрой радиофизики и электроники

Протокол заседания № 09 от «09» июля 2020 г.

И.о. зав. кафедрой



А.В. Бутаков

Программа государственного экзамена составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (утвержден приказом Министерства образования и науки Российской Федерации от 01 декабря 2016 г. №1509)



1. Цель подготовки и сдачи государственного экзамена

Целью подготовки и сдачи государственного экзамена является установление уровня подготовки выпускника к выполнению профессиональных задач и соответствия его подготовки требованиям Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) и основной профессиональной образовательной программы высшего образования (ОПОП ВО) по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализации «Информационная безопасность автоматизированных систем критически важных объектов».

2. Планируемые результаты освоения основной профессиональной образовательной программы

Подготовка и сдача государственного экзамена участвует в формировании у обучающихся компетенций ОК-1-9, ОПК-1-8, ПК-1-28, ПСК-3.1-3.5.

| Компетенции | Планируемые результаты |
|---|--|
| Общекультурные компетенции | |
| ОК-1: способностью использовать основы философских знаний для формирования мировоззренческой позиции | Знать: базовые философские категории и концепции; философское содержание общенаучных методов познания; системного, синергетического и эволюционных подходов в познании явлений действительности Уметь: применять философские знания для изучения естественно-научных и иных дисциплин; проводить философский анализ естественнонаучной информации; формулировать научную проблему в процессе исследовательской деятельности Владеть: методами философского анализа действительности и современных научных концепций; философской и научной методологии в познании природных явлений; философской терминологией и применять ее в обобщении естественнонаучных знаний |
| ОК-2: способностью использовать основы экономических знаний в различных сферах деятельности | Знать: основы экономических знаний в различных сферах деятельности. Уметь: использовать основы экономических знаний в различных сферах деятельности. Владеть: способностью использовать основы экономических знаний в различных сферах деятельности |



| | |
|---|--|
| <p>ОК-3: способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма</p> | <p>Знать: основные этапы и закономерности исторического развития общества.</p> <p>Уметь: анализировать основные этапы и закономерности исторического развития, формулируя собственную точку зрения.</p> <p>Владеть: приемами оценки исторических событий для формирования гражданской позиции</p> |
| <p>ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности</p> | <p>Знать: общие категория и понятия, специальную терминологию основных отраслей права, применяемых на территории Российской Федерации; основные нормативно правовые акты регулирующие профессиональную деятельность.</p> <p>Уметь: использовать основы правовых знаний в различных сферах деятельности.</p> <p>Владеть: навыком применения снов правовых знаний в различных сферах деятельности</p> |
| <p>ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</p> | <p>Знать: Знать основные преимущества своей профессии.</p> <p>Уметь: понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.</p> <p>Владеть: практическими навыками соблюдения норм профессиональной этики.</p> |
| <p>ОК-6: способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия</p> | <p>Знать: принципы функционирования профессионального коллектива, понимать роль корпоративных норм и стандартов; о социальных, этнических, конфессиональных и культурных особенностях представителей тех или иных социальных общностей.</p> <p>Уметь: работать в коллективе, эффективно выполнять задачи профессиональной деятельности; работая в коллективе, учитывать социальные, этнические, конфессиональные, культурные особенности представителей различных социальных общностей в процессе профессионального взаимодействия в коллективе, толерантно воспринимать эти различия.</p> <p>Владеть: приемами взаимодействия с сотрудниками, выполняющими различные профессиональные задачи и обязанности; в процессе работы в коллективе этическими нормами, касающимися социальных, этнических, конфессиональных и культурных различий; способами и приемами предотвращения</p> |



| | |
|---|---|
| | возможных конфликтных ситуаций в процессе профессиональной деятельности. |
| ОК-7: способностью коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности | Знать: базовые категории и понятия в области системы иностранного языка. Уметь: использовать базовые лексико-грамматические средства для общения на иностранном языке. Владеть: навыками осуществления коммуникации в устной и письменной форме на иностранном языках для решения широкого круга задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности. |
| ОК-8: способностью самоорганизации и самообразованию | Знать: содержание процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности. Уметь: планировать цели и устанавливать приоритеты при выборе способов принятия решений с учетом условий, средств, личностных возможностей и временной перспективы достижения; осуществления деятельности; самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности. Владеть: приемами саморегуляции эмоциональных и функциональных состояний при выполнении профессиональной деятельности; технологиями организации процесса самообразования; приемами целеполагания во временной перспективе, способами планирования, организации, самоконтроля и самооценки деятельности. |
| ОК-9: способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности | Знать: основные средства и методы физического воспитания. Уметь: подбирать и применять методы и средства физической культуры для совершенствования основных физических качеств. Владеть: методами и средствами физической культуры для обеспечения полноценной социальной и профессиональной деятельности. |
| Общепрофессиональные компетенции | |



| | |
|---|---|
| <p>ОПК-1: способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач</p> | <p>Знать: особенности организации естественнонаучных исследований; основные правила оформления материалов и результатов лабораторных исследований; правила оформления таблиц, схем, рисунков и чертежей в научных отчетах; правила и способы вычисления погрешностей полученных данных; о размерностях физических величин; базовые теоретические знания по физике; теоретические основы, основные понятия, законы и модели физики; методы и способы получения и освоения материала по физике; о физических процессах, происходящих в окружающем мире и, в частности, о физических процессах, сопровождающих профессиональную деятельность; методы теоретических и экспериментальных исследований в физике; смысл основных терминов и понятий физики.</p> <p>Уметь: эффективно организовать работу по изучению определений и законов естественных наук; грамотно, последовательно и логично оформить результаты работы; пользоваться в профессиональной деятельности теоретическими знаниями и практическими навыками, полученными в рамках изучения физики; понимать, излагать и критически анализировать базовую общефизическую информацию; пользоваться основными понятиями, законами и моделями физики; прогнозировать последствия физических процессов, происходящих в профессиональной деятельности; анализировать полученные экспериментальные данные.</p> <p>Владеть: навыками самостоятельной работы с учебной и научной литературой; базовыми теоретическими знаниями и навыками лабораторных исследований в области физики; использования понятийного аппарата физики в профессиональной деятельности; навыком грамотного представления результатов исследований и навыком оформления отчетов по лабораторным работам; методами обработки и анализа экспериментальной и теоретической физической информации.</p> |
| <p>ОПК-2: способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической</p> | <p>Знать: соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации.</p> <p>Уметь: корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии,</p> |



| | |
|---|---|
| <p>статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p> | <p>дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники. Владеть: навыками решения профессиональных задач, используя соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники.</p> |
| <p>ОПК-3: способностью применять языки, системы и инструментальные средства программирования профессиональной деятельности</p> | <p>Знать: основные способы представления данных и приемы алгоритмизации, функциональные возможности языков программирования различного уровня. Уметь: формализовать поставленную задачу, составлять и оформлять программы на языках программирования. Владеть: навыками работы со средами разработки программ.</p> |
| <p>ОПК-4: способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах</p> | <p>Знать: основные понятия информатики; формы и способы представления данных в персональном компьютере; классификацию современных компьютерных систем; типовые структуры и принципы организации компьютерных сетей. Уметь: пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет. Владеть: навыками поиска информации в глобальной информационной сети Интернет; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией)</p> |
| <p>ОПК-5: способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами</p> | <p>Знать: принципы организации физического эксперимента, приемы и особенности использования измерительной аппаратуры. Уметь: проводить физические эксперименты, фиксировать и обрабатывать результаты измерений, делать выводы из полученных результатов. Владеть: методами анализа достоверности полученных экспериментальных результатов, их соответствия теоретическим представлениям.</p> |



| | | | |
|----------------------|--------|------------------------|---------------|
| Версия документа - 1 | стр. 8 | Первый экземпляр _____ | КОПИЯ № _____ |
|----------------------|--------|------------------------|---------------|

| | |
|---|--|
| <p>ОПК-6: способностью применять нормативные правовые акты в профессиональной деятельности</p> | <p>Знать: основные понятия теории информации и кодирования информация, источники сообщений, каналы связи, коды. Уметь: пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети. Владеть: навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией).</p> |
| <p>ОПК-7: способностью применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций</p> | <p>Знать: основные природные и техногенные опасности, их свойства и характеристики; характер воздействия вредных и опасных факторов на человека и природную среду, методы и способы защиты от них; теоретические основы безопасности жизнедеятельности при ЧС; возможные последствия аварий, катастроф, стихийных бедствий и способы применения современных средств поражения; правовые, нормативно-технические и организационные основы безопасности жизнедеятельности. Уметь: идентифицировать основные опасности среды обитания человека, оценивать риск их реализации; принимать решения по целесообразным действиям в ЧС; распознавать жизненные нарушения при неотложных состояниях и травмах. Владеть: понятийно-терминологическим аппаратом в области безопасности жизнедеятельности; приемами и способами использования индивидуальных средств защиты в ЧС; основными методами защиты производственного персонала и населения при возникновении ЧС; приемами оказания первой помощи пострадавшим в ЧС и экстремальных ситуациях.</p> |
| <p>ОПК-8: способностью к освоению новых образцов программных, технических средств и информационных технологий</p> | <p>Знать: новинки программных, технических средств и информационных технологий. Уметь: осваивать новые образцы программных, технических средств и информационных технологий. Владеть: навыками освоения новых образцов программных, технических средств и информационных технологий.</p> |

Профессиональные компетенции

Научно-исследовательская деятельность

| | |
|--|--|
| <p>ПК-1: способностью осуществлять поиск, изучение, обобщение и</p> | <p>Знать: основные источники получения научно-технической информации, нормативных и</p> |
|--|--|



| | | | |
|----------------------|--------|------------------------|---------------|
| Версия документа - 1 | стр. 9 | Первый экземпляр _____ | КОПИЯ № _____ |
|----------------------|--------|------------------------|---------------|

| | |
|--|---|
| систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке | методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке Уметь: применять действующую законодательную базу в области обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации Владеть: навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках. |
| ПК-2: способностью создавать и исследовать модели автоматизированных систем | Знать: основные принципы построения и исследования моделей автоматизированных систем. Уметь: создавать и исследовать модели автоматизированных систем. Владеть: терминологией и системным подходом построения катастрофоустойчивых ИС. |
| ПК-3: способностью проводить анализ защищенности автоматизированных систем | Знать: основные принципы анализа защищенности автоматизированных систем. Уметь: планировать процедуру анализа защищенности автоматизированных систем. Владеть: средствами проведения анализа защищенности автоматизированных систем. |
| ПК-4: способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы | Знать: основные принципы разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы. Уметь: планировать процесс разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы. Владеть: основными средствами разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы. |
| ПК-5: способностью проводить анализ рисков информационной безопасности автоматизированной системы | Знать: основные принципы анализа рисков информационной безопасности автоматизированной системы. Уметь: планировать процедуру анализа рисков информационной безопасности автоматизированной системы. Владеть: основными средствами проведения анализа рисков информационной безопасности автоматизированной системы. |
| ПК-6: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | Знать: основные принципы проведения анализа и обоснования выбора решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности. Уметь: проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере |



| | | | |
|----------------------|---------|------------------------|---------------|
| Версия документа - 1 | стр. 10 | Первый экземпляр _____ | КОПИЯ № _____ |
|----------------------|---------|------------------------|---------------|

| | |
|---|--|
| | профессиональной деятельности. Владеть: основными средствами для проведения анализа, предложения и обоснования выбора решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности. |
| ПК-7: способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ | Знать: основную входную и выходную научно-техническую документацию. Уметь: разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ. Владеть: средствами сбора информации для подготовки входной и выходной документации по проекту. |
| Проектно-конструкторская деятельность | |
| ПК-8: способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем | Знать: типовые проектные решения по обеспечению безопасности автоматизированных систем. Уметь: разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем. Владеть: программными средствами разработки и анализа проектных решений по обеспечению безопасности автоматизированных систем. |
| ПК-9: способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности | Знать: основные этапы разработки защищенных автоматизированных систем в сфере профессиональной деятельности. Уметь: участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности Владеть: практическими навыками участия в разработке защищенных автоматизированных систем в сфере профессиональной деятельности. |
| ПК-10: способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности | Знать: теорию в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности. Уметь: применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности. Владеть: практическими навыками применения знаний в области электроники и схемотехники, |



| | | | |
|----------------------|---------|------------------------|---------------|
| Версия документа - 1 | стр. 11 | Первый экземпляр _____ | КОПИЯ № _____ |
|----------------------|---------|------------------------|---------------|

| | |
|--|---|
| | технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности. |
| ПК-11: способностью разрабатывать политику информационной безопасности автоматизированной системы | Знать: основные этапы разработки политики информационной безопасности автоматизированной системы. Уметь: разрабатывать политику информационной безопасности автоматизированной системы. Владеть: практическими навыками разработки политики информационной безопасности автоматизированной системы. |
| ПК-12: способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы | Знать: основные этапы проектирования системы управления информационной безопасностью автоматизированной системы. Уметь: участвовать в проектировании системы управления информационной безопасностью автоматизированной системы. Владеть: практическими навыками участия в проектировании системы управления информационной безопасностью автоматизированной системы. |
| ПК-13: способностью участвовать в проектировании средств защиты информации автоматизированной системы | Знать: знать средства защиты информации автоматизированной системы. Уметь: участвовать в проектировании средств защиты информации автоматизированной системы. Владеть: практическими навыками участия в проектировании средств защиты информации автоматизированной системы. |
| Контрольно-аналитическая деятельность | |
| ПК-14: способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации | Знать: факты, принципы, процессы, общие понятия в области применения полученных навыков в рамках реальной практической деятельности. Уметь: на практике применять навыки, полученные при изучении всех предыдущих дисциплин для решения задач по направлению подготовки, составлять детальный план проводимой работы; отбирать и анализировать необходимую информацию по теме работы, готовить аналитический обзор и предпроектный отчет; формулировать выводы по проделанной работе, оформлять законченные проектно-конструкторские работы. Владеть: навыками проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации. |



| | |
|--|---|
| ПК-15: способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем | Знать: основные принципы проведения экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем. Уметь: участвовать в проведении экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем. Владеть: средствами автоматизации проведения экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем. |
| ПК-16: способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации | Знать: основные принципы проведения экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации. Уметь: участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации. Владеть: навыками участия в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации. |
| ПК-17: способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации | Знать: основные этапы инструментального мониторинга защищенности информации в автоматизированной системе и выявления каналов утечки информации. Уметь: проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации. Владеть: автоматизированными средствами проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявления каналов утечки информации. |
| Организационно-управленческая деятельность | |
| ПК-18: способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности | Знать: основные принципы работы малых коллективов исполнителей. Уметь: организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности. Владеть: практическими навыками организации работы малых коллективов исполнителей, выработки и реализации управленческих решений в сфере профессиональной деятельности. |
| ПК-19: способностью разрабатывать предложения по | Знать: основные принципы организации системы управления информационной безопасностью |



| | | | |
|----------------------|---------|------------------------|---------------|
| Версия документа - 1 | стр. 13 | Первый экземпляр _____ | КОПИЯ № _____ |
|----------------------|---------|------------------------|---------------|

| | |
|--|--|
| совершенствованию системы управления информационной безопасностью автоматизированной системы | автоматизированной системы. Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы. Владеть: практическими навыками разработки предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы. |
| ПК-20: способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности | Знать: основные этапы жизни автоматизированной системы с учетом требований информационной безопасности. Уметь: организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности. Владеть: средствами автоматизации разработки, внедрения, эксплуатации и сопровождения автоматизированной системы с учетом требований информационной безопасности. |
| ПК-21: способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем | Знать: основной перечень документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем. Уметь: разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем. Владеть: практическими навыками разработки проектов документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем. |
| ПК-22: способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации | Знать: основные принципы формирования политики информационной безопасности организации и контролировать эффективность ее реализации. Уметь: участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации. Владеть: автоматизированными средствами формирования политики информационной безопасности организации и контролировать эффективность ее реализации. |
| ПК-23: способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа | Знать: правила, процедуры, методы для защиты информации ограниченного доступа. Уметь: формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа. |



| | |
|--|--|
| | Владеть: методами сбора и анализа данных; способностью делать обоснованные заключения на основе полученных результатов; способностью составлять и корректировать план проведения работ в зависимости от полученных результатов. |
| Эксплуатационная деятельность | |
| ПК-24: способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности | Знать: основные информационно-технологические ресурсы автоматизированной системы с учетом требований информационной безопасности. Уметь: обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности. Владеть: практическими навыками эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности. |
| ПК-25: способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций | Знать: основные принципы эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций. Уметь: обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций. Владеть: средствами восстановления работоспособности средств защиты информационно-технологических ресурсов автоматизированной системы при возникновении нештатных ситуаций. |
| ПК-26: способностью администрировать подсистему информационной безопасности автоматизированной системы | Знать: принципы функционирования подсистемы информационной безопасности автоматизированной системы. Уметь: администрировать подсистему информационной безопасности автоматизированной системы. Владеть: автоматизированными средствами администрирования подсистемы информационной безопасности автоматизированной системы. |
| ПК-27: способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы | Знать: этапы работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы. Уметь: выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы |



| | | | |
|----------------------|---------|------------------------|---------------|
| Версия документа - 1 | стр. 15 | Первый экземпляр _____ | КОПИЯ № _____ |
|----------------------|---------|------------------------|---------------|

| | |
|---|---|
| системы | автоматизированной системы. Владеть: автоматизированными средствами осуществления мониторинга и аудита безопасности автоматизированной системы. |
| ПК-28: способностью управлять информационной безопасностью автоматизированной системы | Знать: теорию информационной безопасности автоматизированной системы. Уметь: управлять информационной безопасностью автоматизированной системы. Владеть: методами сбора и анализа данных; способностью делать обоснованные заключения на основе полученных результатов; способностью составлять и корректировать план проведения работ в зависимости от полученных результатов. |
| Профессионально-специализированные компетенции | |
| ПСК-3.1: способностью проводить оценку эффективности средств защиты информации, используемых на критически важных объектах и в автоматизированных системах критически важных объектов | Знать: характеристики основных каналов утечки информации на критически важных объектах. Уметь: проводить оценку эффективности средств защиты информации, используемых на критически важных объектах и в автоматизированных системах критически важных объектов. Владеть: методикой проведения оценки эффективности средств защиты информации, используемых на критически важных объектах и в автоматизированных системах критически важных объектов. |
| ПСК-3.2: способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, используемых на критически важных объектах и в автоматизированных системах критически важных объектов | Знать: средства защиты информации, используемые на критически важных объектах. Уметь: участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, используемых на критически важных объектах и в автоматизированных системах критически важных объектов. Владеть: навыками разработки, внедрения и эксплуатации средств защиты информации, используемых на критически важных объектах и в автоматизированных системах критически важных объектов. |
| ПСК-3.3: способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов | Знать: современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов. Уметь: применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов. |



| | |
|---|---|
| | Владеть: навыками применения современной нормативной базы, регламентирующей деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов. |
| ПСК-3.4: способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов | Знать: способы и средства охраны объектов. Уметь: разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов. Владеть: навыками разработки технических регламентов для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов. |
| ПСК-3.5: способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и автоматизированных системах критически важных объектов | Знать: терминологию и системный подход к построению защищенных автоматизированных систем критически важных объектов. Уметь: проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и автоматизированных системах критически важных объектов. Владеть: навыками проектирования, внедрения и использования системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов. |

3. Трудоемкость, порядок и форма государственного экзамена

Трудоемкость подготовки и сдачи государственного экзамена – 108 часов (3 зачетные единицы).

В соответствии с учебным планом – 10-ой семестр.

Кафедра не позднее, чем за полгода до проведения экзамена доводит до сведения студентов перечень вопросов, вынесенных на экзамен, список рекомендованной литературы путем размещения их в соответствующем разделе на сайте Университета.

Декан факультета не позднее, чем за тридцать дней до проведения государственного экзамена, разрабатывает проект расписания государственных аттестационных испытаний, в котором указываются даты, время и место проведения государственных аттестационных испытаний и



предэкзаменационных консультаций. Проект расписание согласуется с УОП и утверждается проректором по учебной работе. Утвержденное расписание доводится до сведения обучающихся, председателей и членов государственных экзаменационных комиссий.

Не позднее недельного срока до государственного экзамена проводится предэкзаменационная консультация для обучающихся, на которой разъясняется порядок сдачи государственного экзамена, права и обязанности обучающихся, разбираются наиболее сложные для понимания разделы программы.

Порядок проведения государственного экзамена: Аттестационное испытание проводится в форме устного экзамена с оформлением письменного листа устного ответа. Студенты должны в отдельной аудитории в течение двух академических часов ответить на вопросы экзаменационного билета. При этом они должны продемонстрировать знание физических и радиофизических понятий, явлений, законов и теорий; понимание их физического смысла; знания, относящиеся к актуальным, современным аспектам вопроса, а также продемонстрировать навыки владения этими знаниями в ходе устного ответа с экзаменаторами.

Для проведения государственного экзамена на основании содержания программы государственного экзамена формируются экзаменационные билеты. Экзаменационный билет содержит два теоретических вопроса.

Перечень вопросов государственного экзамена ежегодно обновляется, обсуждается и утверждается на выпускающей кафедре.

4. Вопросы к государственному экзамену

4.1. Математический анализ

1. Множество действительных чисел. Принцип точной верхней грани. Аксиома Архимеда.
2. Предел последовательности и его свойства.
3. Критерий Коши сходимости последовательностей.
4. Критерий Вейерштрасса. Число e .
5. Подпоследовательности. Верхний и нижний пределы последовательности.
6. Предел функции в точке и его свойства.
7. Предел функции и арифметические операции. Предел функции и неравенства. Предел композиции функций.
8. Критерий Коши существования предела функции.
9. Замечательные пределы и эквивалентные функции.



10. Односторонние пределы. Локальные свойства непрерывных функций. Классификация разрывов.
11. Глобальные свойства непрерывных функций.
12. Множества и отображения.
13. Элементарные функции.
14. Производная функции и ее свойства.
15. Основные теоремы о дифференцируемых функциях.
16. Формула Тейлора.
17. Достаточное условие экстремума. Выпуклость и вогнутость функции.
18. Правило Лопиталю.
19. Первообразная и неопределенный интеграл и его свойства.
20. Простейшие приемы интегрирования.
21. Интегрирование рациональных функций.
22. Метод Остроградского.
23. Интегрирование некоторых иррациональных функций.
24. Интегрирование тригонометрических функций
25. Подстановки Эйлера
26. Определение собственного интеграла Римана и интегралов Дарбу. Их связь.
27. Свойства интеграла Римана.
28. Интеграл как функция верхнего предела. Формула Ньютона-Лейбница.
29. Интегрирование рациональных функций.
30. Интегрирование некоторых иррациональных функций.
31. Интегрирование некоторых трансцендентных функций.
32. Свойства открытых и замкнутых множеств
33. Свойства компактных множеств
34. Критерий компактности
35. Локальные свойства непрерывных функций
36. Глобальные свойства непрерывных функций
37. Достаточное условие дифференцируемости
38. Матрица Якоби
39. Локальные свойства дифференцируемых функций
40. Локальный экстремум
41. Теорема о неявной функции
41. Сумма и сходимость числового ряда. Критерий Коши сходимости ряда. Необходимый признак сходимости.
42. Свойства сходящихся рядов. Абсолютно и условно сходящиеся ряды.
43. Ряды с неотрицательными членами. Критерий Вейерштрасса. Признаки
44. сравнения.
45. Обобщенный гармонический ряд.



46. Признаки сходимости Даламбера, Коши. Ряды Лейбница. Признаки Абеля и Дирихле.
47. Теорема Коши об абсолютно сходящихся рядах. Теорема Римана об условно сходящихся рядах.

4.2. Теория вероятностей и математическая статистика

1. Статистическое определение вероятностей.
2. Алгебра событий и пространство элементарных событий.
3. Классическое определение вероятности.
4. Важнейшие свойства вероятности и простейшие формулы.
5. Условная вероятность. Формула умножения. Независимость событий.
6. Формула полной вероятности.
7. Формула Байеса.
8. Испытания Бернулли.
9. Формула Бернулли.
10. Формула Пуассона.
11. Теорема Бернулли.
12. Геометрическая вероятность.
13. Дискретные случайные величины и их распределения.
14. Пуассоновский поток событий.
15. Функция распределения вероятностей и ее свойства.
16. Плотность распределения вероятностей.
17. Математическое ожидание.
18. Дисперсия.
19. Многомерные случайные величины.
20. Преобразование случайных величин.
21. Закон больших чисел.
22. Центральная предельная теорема.
23. Понятие выборки. Выборочное среднее, выборочная дисперсия, выборочные моменты.
24. Эмпирическая функция распределения.
25. Понятие оценки параметров распределения. Свойства оценок: состоятельность, несмещенность, эффективность.
26. Методы построения оценок. Метод моментов.
27. Метод наибольшего правдоподобия.
28. Неравенство Рао-Крамера.
29. Доверительные интервалы.
30. Алгоритм построения доверительных интервалов.
31. Доверительный интервал параметров нормального распределения
32. Понятие статистической гипотезы. Основные этапы проверки гипотез.



33. Проверка гипотез о числовых значениях параметров различных распределений (нормальное, распределение Стьюдента).
34. Критерий хи-квадрат.
35. Критерий Колмогорова

4.3. Алгебра

1. Алгебраические операции. Ассоциативные, коммутативные операции, нейтральные элементы.
2. Определение группы, примеры групп, свойства группы, симметрическая группа.
3. Определение кольца, примеры колец.
4. Определение поля, примеры полей. Характеристика поля. Теорема о характеристике.
5. Построение поля комплексных чисел.
6. Свойства сопряжение комплексных чисел.
7. Тригонометрическая форма комплексного числа, формула Муавра.
8. Корни из комплексного числа, теорема о корнях из единицы.
9. Понятия матрицы, операции над матрицами. Теорема о свойствах сложения матриц и умножения матрицы на элемент кольца.
10. Произведение матриц. Теорема о свойствах произведения матриц.
11. Понятие обратимости матриц. Примеры обратимых и необратимых матриц над кольцами. Теорема о свойствах обратимых матриц.
12. Доказать, что обратимые матрицы над кольцом образуют группу по умножению.
13. Понятие транспонирования матрицы. Теорема о свойствах транспонирования матриц.
14. Понятия подстановки и перестановки. Четность перестановок и подстановок. Доказать, что транспозиция меняет четность перестановки.
15. Два определения определителя и их равносильность.
16. Теорема об определителе транспонированной матрицы. О равноправии строк и столбцов в определителе.
17. Теорема об определителе полураспавшейся матрицы.
18. Теорема об определителе треугольной матрицы.
19. Теорема о кососимметричности определителя.
20. Теорема о линейности определителя.
21. Миноры и алгебраические дополнения. Теорема о свойствах алгебраических дополнений. Разложение определителя по строчке и столбцу.
22. Понятие присоединенной матрицы. Теорема о присоединенной матрице.
23. Теорема об определителе произведения двух матриц.
24. Теорема об обратной матрице.



25. Определитель Вандермонда и циркулянт.
26. Вычисление обратной матрицы с помощью элементарных преобразований строк. Обоснование метода.
27. Понятие решения системы линейных уравнений, совместные и несовместные системы. Теорема об элементарных преобразованиях.
28. Алгоритм Гаусса и следствия из него.
29. Теорема Крамера.
30. Построение кольца многочленов от одного неизвестного.
31. Кольца без делителей нуля. Примеры.
32. Теорема о делении с остатком в кольце многочленов и в кольце целых чисел.
33. Свойства делимости многочленов и целых чисел.
34. Наибольший общий делитель для многочленов, его свойства, алгоритм Евклида для многочленов.
35. Теорема о линейном представлении наибольшего общего делителя.
36. Взаимно простые многочлены и их свойства.
37. Неприводимость многочленов, основная теорема арифметики многочленов.
38. Понятие производной многочлена. Теорема о кратных множителях многочлена и его производной. Отделение кратных множителей многочлена с помощью алгоритма Евклида.
39. Корни многочленов. Теорема Безу. Схема Горнера.
40. Теорема о числе корней и степени многочлена.
41. Функциональное и алгебраическое равенство многочленов. Теорема об однозначности задания многочлена своими значениями.
42. Интерполяционные формулы Лагранжа и Ньютона.
43. Решение уравнений третьей и четвертой степени.
44. Построение кольца многочленов от нескольких неизвестных.
45. Симметрические многочлены, формулы Виета.
46. Основная теорема о симметрических многочленах.
47. Теорема о существовании корня неприводимого многочлена в некотором расширении поля и следствие из нее.
48. Основная теорема алгебры многочленов.
49. Рациональные корни многочленов над полем рациональных чисел.
50. Определение векторного пространства. Простейшие свойства векторных пространств.
51. Определение подпространства, основные свойства подпространства.
52. Определение линейной зависимости и линейной независимости векторов, свойства линейно зависимых и независимых векторов.
53. Критерий линейной зависимости.



54. Теорема об очистке линейно полного множества, определение базиса.
55. Теорема о выборе базиса.
56. Теорема о дополнении до базиса.
57. Критерий базиса.
58. Определение координат вектора в базисе, свойства координат вектора.
59. Размерность пространства, теорема о размерности, следствия из нее.
60. Матрица перехода, свойства матрицы перехода.
61. Теорема о монотонности размерности подпространств.
62. Теорема о пересечении подпространств.
63. Линейная оболочка, теорема о линейной оболочке.
64. Сумма подпространств, теорема о сумме подпространств.
65. Теорема о размерности суммы подпространств.
66. Прямая сумма подпространств, теорема о прямой сумме подпространств.
67. Дополнение к подпространству, теорема о существовании дополнения к подпространству.
68. Прямая сумма пространств, теорема о прямой сумме пространств.
69. Три понятия ранга матрицы, доказать, что строчный ранг матрицы не изменяется при элементарных преобразованиях строк.
70. Доказать, что столбцовый ранг матрицы не изменяется при элементарных преобразованиях столбцов.
71. Доказать, что строчный ранг матрицы не изменяется при элементарных преобразованиях столбцов.
72. Доказать, что столбцовый ранг матрицы не изменяется при элементарных преобразованиях строк.
73. Доказать, что столбцовый ранг матрицы равен строчному рангу матрицы.
74. Доказать, что при элементарных преобразованиях строк минорный ранг матрицы не меняется.
75. Теорема Кронекера-Капелли.
76. Теорема об описании структуры решений системы линейных уравнений.
77. Теорема о размерности пространства решений системы линейных однородных уравнений.
78. Определение линейного оператора, теорема о свойствах линейных операторов.
79. Операции над линейными операторами, теорема о свойствах операций над линейными операторами.
80. Теорема о задании линейного оператора на базисе и матрицей.
81. Теорема о свойствах матриц линейных операторов.
82. Линейные функционалы.
83. Линейные преобразования пространства .
84. Матрицы линейных преобразований в разных базисах.



85. Определение определителя матрицы линейного преобразования, доказать, что определитель линейного преобразования определен корректно.
86. Инвариантные подпространства, свойства инвариантных подпространств.
87. Характеристический многочлен линейного преобразования, теорема о характеристическом многочлене.
88. Теорема Гамильтона-Кэли.
89. Собственные векторы и собственные значения, теорема о нахождении собственных значений.
90. Теорема об одномерных инвариантных подпространствах.
91. Доказать, что собственные векторы, соответствующие различным собственным значениям линейно независимы.
92. Пространства со скалярным произведением, простейшие свойства таких пространств.
93. Теорема Коши-Буняковского-Шварца.
94. Свойства нормы вектора.
95. Ортогональность векторов и подпространств, теорема об ортогональных множествах векторов, процесс ортогонализации Грама-Шмидта.
96. Ортогональное дополнение, теорема об ортогональном дополнении.
97. Теорема о связи между ортонормированными базисами в пространстве со скалярным произведением.
98. Линейные функционалы, теорема о линейном функционале на пространстве со скалярным произведением.
99. Сопряженное преобразование, теорема существования сопряженного преобразования.
100. Теорема о свойствах сопряженных преобразований.
101. Теорема о матрице сопряженного преобразования.
102. Нормальные преобразования, теорема о собственных векторах и собственных значениях нормального преобразования.
103. Критерий сохранения скалярного произведения линейным преобразованием.
104. Два понятия квадратичной формы (как функции и как многочлена), связь между ними.
105. Теорема о матрице квадратичной формы.
106. Теорема Лагранжа о приведении квадратичной формы к каноническому виду.
107. Теорема о приведении квадратичной формы к диагональному виду с помощью перехода к ортонормированному базису.
108. Закон инерции квадратичных форм.
109. Линейная классификация квадратичных форм.
110. Критерий положительной определенности квадратичных форм.



111. Критерий Сильвестра.

4.4. Теория информации

1. Информационные характеристики дискретных вероятностных схем: энтропия, условная энтропия.
2. Виды информации: собственная информация, взаимная информация, Условная информация.
3. Источник сообщений как случайный процесс, дискретный источник сообщений.
4. Код над алфавитом, кодирование источника сообщений. Код Шеннона-Фано.
 1. Средняя длина неравномерного кодирования.
5. Префиксный код. Неравенство Крафта. Критерий существования префиксного кода.
6. Скорость создания информации. Прямая и обратная теоремы кодирования Шеннона.
7. Оптимальный неравномерный код Хаффмана.
8. Что значит задать дискретный канал без памяти (ДКБП)? Описание двоичного симметричного канала (ДСК). Код канала. Скорость канала. Процесс декодирования. Средняя вероятность ошибки.
9. Пропускная способность дискретного канала. Количество взаимной информации между событиями. Средняя взаимная информация.
10. Информационная емкость дискретного канала без памяти. Прямая и обратная теоремы кодирования для ДСК. Линейный код над двоичным полем. Порождающая и проверочная матрица. Систематический код.
11. Расстояние Хемминга, теорема Хэмминга. Декодирование по минимуму расстояния Хэмминга. Синдромное декодирование.
12. Линейные коды Хэмминга. Совершенные коды. Граница Хэмминга для двоичных кодов.
13. Верхняя граница Плоткина. Нижняя граница Варшамого-Гилберта.
14. Декодирование по минимуму вероятности ошибки и декодирование по максимуму правдоподобия. Вероятность ошибки декодирования в ДСК каналах.
15. Циклические коды. Порождающий многочлен. Критерий существования циклического кода с заданным порождающим многочленом. Проверочный многочлен. Систематическое кодирование циклическими кодами.
16. Многочлен ошибок Синдромный многочлен. Синдромное декодирование циклических кодов.



17. Порождающая и проверочная матрица циклического кода.
Циклический код Хэмминга.

4.5. Языки программирования

1. История развития языков программирования.
2. Языки программирования. Основные понятия и определения. Классификация.
3. Модель передачи сообщения.
4. Основные позиции при изучении языков программирования.
5. Сложность как основная проблема программирования, её источники и средства борьбы с нею.
6. Разновидности программирования.
7. Понятие о базовом языке.
8. Немного истории. Язык С. Философия программирования, заложенная в языке С. ООП. Обобщённое программирование. Язык С++.
9. Переносимость и стандарты.
10. Методика создания программ. Создание исходного кода. Компиляция и компоновка.
11. Начальные сведения о языке С++. Функция main(). Комментарии в языке С++. Препроцессор С++ и файл iostream. Имена заголовочных файлов. Области имён. Вывод данных в языке С++ с использованием объекта cout. Форматирование исходного кода.
12. Краткие сведения об операторах языка С++. Операторы объявления и переменные. Оператор присваивания. Применение объекта cin. Классы.
13. Функции. Применение функций с возвращаемым значением. Разновидности функций. Функции, определяемые пользователем.
14. Простые переменные. Имена переменных. Всё обо всех целочисленных типах данных.
15. Квалификатор const. Числа с плавающей точкой. Всё обо всех типах данных с плавающей точкой.
16. Арифметические операции языка С++. Приоритет операций и ассоциативность. Разновидности операций деления. Операция деления по модулю. Преобразования типов данных.
17. Всё о массивах и строках.
18. Всё о структурах, объединениях, перечислениях.
19. Всё об указателях. Операторы new и delete. Автоматическая, статическая и свободная память.
20. Цикл for и его возможности.
21. Выражения сравнения.
22. Цикл while.



4.6 Технологии и методы программирования

1. Статические и динамические структуры данных, их сравнение. Примеры.
2. Структура данных стек. Способы реализации. Примеры использования: вычисление символьных выражений.
3. Структура данных стек. Способы реализации. Примеры использования: алгоритм Грехэма построения выпуклой оболочки.
4. Структуры данных очередь, дек и список. Способы реализации. Примеры использования: построение эйлера пути в графе.
5. Структуры данных очередь, дек и список. Способы реализации. Примеры использования: перечисление чисел с заданными простыми делителями.
6. Структура данных дерево. Виды деревьев. Способы реализации и хранения.
7. Структура данных дерево. Красно-черные деревья. Определение, теорема о сбалансированности.
8. Структура данных дерево. Красно-черные деревья. Операция вставки элемента.
9. Сложность алгоритма. Критерии оценки эффективности алгоритмов. Факторы, влияющие на производительность.
10. Методы анализа алгоритмов. Метод производящих функций. Пример расчетов для алгоритма поиска максимального элемента массива.
11. Методы анализа алгоритмов. Расчет сложности алгоритма из рекуррентного соотношения. Пример использования: быстрое умножение длинных чисел и алгоритм Штрассена.
12. Алгоритмы внутренней сортировки. Элементарные операции, их влияние на производительность алгоритма. Теорема о производительности алгоритма внутренней сортировки с помощью сравнений.
13. Простейшие алгоритмы внутренней сортировки. Оценка их сложности, сравнение.
14. Эффективные алгоритмы внутренней сортировки. Пирамидальная сортировка.
15. Эффективные алгоритмы внутренней сортировки. Быстрая сортировка. Нахождение медианы и k-ого по величине элемента.
16. Эффективные алгоритмы внутренней сортировки. Карманная сортировка.
17. Алгоритмы поиска данных. Хеширование. Хеш-функции, требования к хе-шу, примеры.



18. Алгоритмы поиска данных. Хеширование. Разрешение коллизий с помощью цепочек. Открытая адресация.
19. Поиск подстрок в строках. Формулировка задачи. Основные определения. Простейший алгоритм.
20. Поиск подстрок в строках. Алгоритм Рабина-Карпа. Выбор хеш-функции в алгоритме Рабина-Карпа.
21. Поиск подстрок в строках. Поиск с помощью конечного автомата. Построение функции перехода. Анализ сложности алгоритма.
22. Поиск подстрок в строках. Алгоритм Кнута-Морриса-Пратта. Построение префикс-функции. Анализ сложности алгоритма.

4.7. Криптографические методы защиты информации

1. Алгоритм Диффи-Хеллмана. Задача Диффи-Хеллмана. Задача дискретного логарифмирования.
2. Криптосистема RSA (шифрование, расшифрование, корректность). Задача RSA.
3. Атаки на RSA
4. Алгоритмы факторизации:
5. Выбор параметров криптосистемы RSA. Генерация сильно простых чисел методом Гордона. Использование китайской теоремы об остатках в RSA.
6. Схема шифрования RSA-OAEP.
7. Криптосистемы с открытым ключом.
 - система Голдвассера-Микали;
 - рюкзачный метод шифрования Меркла Хеллмана;
 - система Эль-Гамала;
 - система Рабина;
 - система Мак-Элиса.
8. Алгоритмы дискретного логарифмирования:
 - метод больших и малых шагов;
 - метод Полларда;
 - индекс метод;
 - метод Полига Хеллмана.
9. Хеш-функции. Требования. Предназначение. Модель Меркле-Дамгарда. Функция губки (sponge function).
10. Стандарты хеш-функций.
11. Общая схема алгоритмов MD4, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94.
12. Криптоанализ хеш-функций. Модель случайного оракула (ROM).
Атака на основе парадокса дней рождений:
 - метод Полларда;
 - метод Полларда.



- метод Хеллмана;
- радужные таблицы.
- 13. Электронная цифровая подпись (ЭЦП). Задачи ЭЦП.
- 14. Схема ЭЦП Диффи-Лампорта. Вероятностная схема ЭЦП Рабина.
- 15. Схема ЭЦП Эль-Гамала. Уменьшение размера подписи в схеме Эль-Гамала.
- 16. ЭЦП DSA.
- 17. ЭЦП ГОСТ Р 34.10-94.
- 18. ЭЦП Онга-Шнорра-Шамира.
- 19. ЭЦП Шнорра.
- 20. Схемы ЭЦП с восстановлением сообщений (на основе RSA, на основе ЭЦП Эль-Гамала, ЭЦП Рабина).
- 21. Слепая ЭЦП Чаума (на основе RSA).

4.8. Основы информационной безопасности

1. Понятие национальной безопасности. Основные угрозы национальной безопасности России.
2. Интересы личности, общества и государства в информационной сфере. Понятие информационной безопасности
3. Основные положения государственной политики и организационная основа обеспечения информационной безопасности РФ.
4. Виды угроз информационной безопасности Российской Федерации.
5. Источники угроз информационной безопасности Российской Федерации.
6. Информационная безопасность и информационное противоборство.
7. Понятие информационной войны, цели и средства её ведения
8. Информационное оружие, его классификация и возможности.
9. Понятие кибертерроризма
10. Основные направления обеспечения информационной безопасности объектов информационной инфраструктуры государства
11. Общие принципы и методы обеспечения информационной безопасности Российской Федерации.
12. Конституция РФ о правах и обязанностях граждан в информационной сфере
13. Виды защищаемой информации.
14. Правовой режим защиты государственной тайны.
15. Правовой режим защиты коммерческой тайны.
16. Правовой режим защиты персональных данных.
17. Уголовная ответственность за компьютерные преступления.
18. Понятие и виды административной ответственности за нарушение требований информационной безопасности.



19. Методы и средства обеспечения безопасности компьютерных систем.
20. Обязанности обладателя конфиденциальной информации по ее защите.
21. Политика обеспечения информационной безопасности.
22. Конфиденциальные документы: состав, сроки, реквизиты. Угрозы конфиденциальному документу.
23. Контроль и надзор в сфере обеспечения информационной безопасности.
24. Понятие и уровни защищенности автоматизированных информационных систем (АИС).
25. Основные требования по защите АИС
26. Состав и содержание организационных и технических мер по защите АИС
27. Процедура оценки обстановки на объекте защиты
28. Базовые и частные модели угроз безопасности АИС
29. Методика оценки актуальности угроз безопасности АИС.
30. Этапы создания и структура службы безопасности предприятия.
31. Задачи подразделения информационной безопасности предприятия.
32. Должностные обязанности руководителя подразделения информационной безопасности.
33. Должностные обязанности администратора безопасности АИС.
34. Обязанности пользователя АИС по обеспечению информационной безопасности.

4.9. Операционные системы

1. Понятие операционной системы (Поколения ОС. Классификация ОС. Интерфейсы ОС.)
2. Основные принципы работы многозадачных и многопользовательских ОС.
3. Управление ресурсами: виды и иерархия ресурсов, виртуальные ресурсы, понятия стратегии и дисциплины управления ресурсами.
4. Управление процессорами: режимы работы, обработка прерываний.
5. Управление памятью, управление данными и устройствами.
6. Аппаратная поддержка работы ОС.
7. Управление процессами.
8. Модель процесса. Состояния процессов Создание и завершение процесса.
9. Реализация процессов. Модель потока. Нити.
10. Принципы организации многонитового процесса. Реализация нитей.
11. Планирование процессов. Категории и критерии качества алгоритмов планирования.
12. Планирование в интерактивных системах. Алгоритмы планирования.
13. Приоритетное планирование. Гарантированное планирование. Многоуровневое планирование.



14. Взаимодействие между процессами.
15. Взаимодействие процессов. Организация обмена данными. Средства обмена данными.
16. Характеристики средств связи.
17. Передача информации с помощью каналов связи.
18. Организация взаимодействия процессов в UNIX.
19. Механизмы IPC и общие принципы их организации.
20. Конфликты и состояния состязания.
21. Взаимное исключение. Критические области.
22. Алгоритмы синхронизации процессов. Условия корректности алгоритмов синхронизации.
23. Взаимное исключение с активным ожиданием. Недостатки алгоритмов с активным ожиданием.
24. Семафоры. Мониторы. Сообщения.
25. Основное управление памятью.
26. Многозадачность с фиксированными разделами.
27. Многозадачность с переменными разделами.
28. Подкачка. Виртуальная память. Страничная организация памяти.
29. Таблицы страниц. Структура элемента таблицы страниц. Методы организации таблиц.
30. Буфер быстрого преобразования адреса (TLB).
31. Алгоритмы замещения страниц.
32. Пробуксовка.
33. Рабочее множество.
34. Замещение страниц в многозадачной среде.
35. Сегментная организация памяти.
36. Сегментно-страничная организация памяти.

4.10. Безопасность систем баз данных

- 1) Информация. Информационная система. История и причины возникновения.
- 2) Свойства баз данных. Критерии применения баз данных. Примеры современных автоматизированных информационных систем с базами данных.
- 3) Определение СУБД. Основные функции СУБД.
- 4) Классификация СУБД по типу базы данных, по архитектуре СУБД и способу хранения данных, по способу к данным.
- 5) Особенности, достоинства и недостатки СУБД.
- 6) Подходы к проектированию баз данных: инфологическое, логическое, даталогическое, физическое.



- 7) Концептуальная модель данных, физическая модель данных.
- 8) Двухзвенная архитектура автоматизированной информационной системы, трехзвенная архитектура автоматизированной информационной системы.
- 9) SQL. Нормализация базы данных, описание и примеры нормальных форм.
- 10) Безопасность информации и информационная безопасность. Информация и информационный процесс.
- 11) Свойства информации, обеспечиваемые при её защите.
- 12) Угрозы и уязвимости информационной безопасности.
- 13) Привилегии основных ролей и пользователей.
- 14) Иерархия безопасности.
- 15) Инструкции по распределению прав пользователей.
- 16) Принудительный контроль доступа к объектам базы данных.
- 17) Модели управления доступом. Дискреционная модель.
- 18) Ролевая модель. Мандатная модель.
- 19) Логическая и физическая целостность данных.
- 20) Правила ограничения целостности данных, журналы транзакций, откат изменений по журналу транзакций.
- 21) Определение и задачи распределенных систем.
- 22) Транзакции и свойства транзакций. Журналы транзакций, откат изменений по журналу транзакций.

4.11. Безопасность сетей ЭВМ

- 1) История развития сетей ЭВМ. Место и роль вычислительных сетей в современном мире.
- 2) Основные понятия и терминология. Общие представления о вычислительной сети. Общее понятие об иерархической структуре протоколов.
- 3) Принципы многоуровневой организации локальных и глобальных сетей ЭВМ. Модель OSI.
- 4) Стандартные стеки коммуникационных протоколов.
- 5) Стандартизация в сетях. Классификация вычислительных сетей.
- 6) Требования, предъявляемые к современным вычислительным сетям.
- 7) Методы и технологии проектирования средств телекоммуникаций. Структуризации сети.
- 8) Физическая и логическая топологии сетей.
- 9) Основное коммуникационное оборудование.
- 10) Каналы связи. Характеристики каналов связи.
- 11) Логическое кодирование.
- 12) Асинхронная и синхронная передачи.
- 13) Иерархия в кабельной системе. Структурированная кабельная система.



- 14) Конфигурации локальных вычислительных сетей и методы доступа в них. Структура и функции локальных сетей.
- 15) Содержание стандарта IEEE 802. Базовые технологии локальных сетей. IEEE 802.2 Ethernet. Оборудование локальных сетей.
- 16) Программные средства телекоммуникации.
- 17) Структура программного обеспечения локальной сети.
- 18) Классификация программного обеспечения локальных сетей.
- 19) Принципы построения сетевого программного обеспечения и сетевых операционных систем.
- 20) Классификация серверов. Проектирование сетей ЭВМ по принципу «клиент-сервер».
- 21) Сетевой уровень передачи данных. IP-адресация.
- 22) Реализация межсетевого взаимодействия средствами TCP/IP. Порядок распределения IP-адресов. Отображение IP-адресов на локальные адреса.
- 23) ARP протокол.
- 24) Принципы маршрутизации в IP-сетях. Протоколы маршрутизации.
- 25) Понятие домена. Доменная адресация в IP-сетях.
- 26) DNS протокол. Протокол IPv6. Протоколы транспортного уровня TCP и UDP.
- 27) Современные тенденции развития телекоммуникационных систем.
- 28) Интеграция различных типов сетей и сетевых служб.
- 29) Виртуализация информационных систем.
- 30) Облачные вычисления.
- 31) Обеспечение безопасности телекоммуникационных связей и административный контроль.
- 32) Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность.
- 33) Защита топологии сети.
- 34) Виртуальные локальные сети. Дополнительные функции коммутаторов. Персональные экраны.
- 35) Абонентское шифрование. Защита сетевого трафика и компонентов сети.
- 36) Защита компонентов сети от НСД. Безопасность ресурсов сети.
- 37) Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
- 38) Средства повышения надежности функционирования сетей.
- 39) Регламентирующие документы в области безопасности вычислительных сетей. Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.



- 40) Сетевые операционные системы Windows, Unix/Linux. Основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля.
- 41) Понятие политики безопасности. Типовые элементы политики безопасности. Построение, реализация, поддержание и модификация политики безопасности.
- 42) Критерии оценки безопасности сетевых ОС. Основные критерии анализа сетевой безопасности. Общая процедура анализа.
- 43) Основные механизмы обеспечения безопасности и управления распределенными ресурсами.
- 44) Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи.
- 45) Использование межсетевых экранов. Виртуальные частные сети.
- 46) Уязвимости и защита базовых протоколов и служб. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты.
- 47) Системы обнаружения и противодействия вторжениям.
- 48) Классификация и принципы функционирования систем обнаружения вторжений.
- 49) Сканеры безопасности. Классы сканеров безопасности и особенности применения.
- 50) Защита от вирусов. Защита электронного документооборота.

4.12. Программно-аппаратные средства обеспечения информационной безопасности

- 1) Понятие политики безопасности. Описание типовых политик безопасности.
- 2) Угрозы безопасности компьютерных систем. Модель компьютерной системы.
- 3) Понятие монитора безопасности. Концепция диспетчера доступа.
- 4) Обеспечение гарантий выполнения политики безопасности.
- 5) Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности.
- 6) Модели безопасного взаимодействия в КС.
- 7) Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.
- 8) Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.
- 9) Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности.



- 11) Взаимодействие с общесистемными компонентами вычислительных систем.
- 12) Методы и средства ограничения доступа к компонентам вычислительных систем.
- 13) Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
- 14) Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации.
- 15) Защита программ от изучения.
- 16) Способы встраивания средств защиты в программное обеспечение.
- 17) Защита от разрушающих программных воздействий и вредоносного программного обеспечения.
- 18) Защита программ от изменения и контроль целостности.
- 19) Роль стандартов информационной безопасности. Документы Государственной технической комиссии России.
- 20) Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
- 21) Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
- 22) Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем.
- 23) Требования к процессу сертификации продукта информационных технологий

Фонды оценочных средств дисциплин и ГИА прилагаются.

5. Критерии оценивания государственного экзамена

Оценка за государственный экзамен выставляется по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» ставится обучающимся, которые при ответе обнаруживают систематическое и глубокое знание материала; владеют терминологией, понятийным аппаратом; демонстрируют способность к анализу и сопоставлению различных подходов. Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений, при этом делаются обоснованные выводы. Ответ обучающегося на вопросы билета и вопросы членов экзаменационной



комиссии является развернутым, уверенным и содержит достаточно четкие формулировки.

Оценка «хорошо» ставится обучающимся, которые при ответе: обнаруживают твердое знание материала, но допускают отдельные погрешности и неточности при ответе на вопросы билета и вопросы членов экзаменационной комиссии. Материал излагается последовательно и уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер.

Оценка «удовлетворительно» ставится обучающимся, которые при ответе показывают знание основного материала, но допускают существенные погрешности в ответе на вопросы экзаменационного билета и вопросы членов экзаменационной комиссии; приводимые в ответе формулировки являются недостаточно четкими, в ответах допускаются неточности. Демонстрируются поверхностное знание вопроса. Имеются затруднения с выводами.

Оценка «неудовлетворительно» ставится обучающимся, которые при ответе: обнаруживают значительные пробелы в знаниях основного материала; допускают принципиальные ошибки в ответе на вопрос билета; демонстрируют незнание теории; не умеет применять теоретические знания на практике. Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний. Обучающийся не ответил на вопросы билета или членов экзаменационной комиссии.

6. Учебно-методическое обеспечение

Основная литература

1. Бермант, А. Ф. Краткий курс математического анализа [Текст]: учебное пособие / А. Ф. Бермант, И. Г. Араманович. — 14-е изд., стер. — Санкт-Петербург : Лань, 2008. — 736 с.: ил. — (Учебники для вузов. Специальная литература) (Классическая учебная литература по математике) (Лучшие классические учебники) (Знание. Уверенность. Успех!). — Библиогр.: с. 736. — ISBN 978-5-8114-0499-5.
2. Гмурман, В. Е. Теория вероятностей и математическая статистика [Электронный ресурс]: учебник / В. Е. Гмурман. — 12-е изд. — Москва: Юрайт, 2017. — 479 с. — (Профессиональное образование). — Режим доступа: <https://www.biblio-online.ru>. — Internet access. — ISBN 978-5-534-00859-3. — URL: <https://www.biblio-online.ru/bcode/399289>.
3. Кострикин, А. И. Введение в алгебру [Электронный ресурс]: учебник. 1. Основы алгебры / А.И. Кострикин. — Москва: МЦНМО, 2009. — 273 с. —



- <http://biblioclub.ru/>. — ISBN 978-5-94057-453-8. —
URL: <http://biblioclub.ru/index.php?page=book&id=63140>.
4. Кострикин, А. И. Введение в алгебру [Электронный ресурс]: учебник. 2. Линейная алгебра / А.И. Кострикин. — Москва : МЦНМО, 2009. — 368 с. —
<http://biblioclub.ru/>. — ISBN 978-5-94057-454-5. —
URL: <http://biblioclub.ru/index.php?page=book&id=63144>.
5. Кострикин, А. И. Введение в алгебру [Электронный ресурс]: учебник. 3. Основные структуры алгебры / А.И. Кострикин. — Москва: МЦНМО, 2009. — 272 с. —
<http://biblioclub.ru/>. — ISBN 978-5-94057-455-2. —
URL: <http://biblioclub.ru/index.php?page=book&id=62951>.
6. Кудряшов, Б. Д. Теория информации [Электронный ресурс] / Кудряшов Б. Д. — Санкт-Петербург: НИУ ИТМО, 2010. — 188 с. — Книга из коллекции НИУ ИТМО - Информатика. —
URL: http://e.lanbook.com/books/element.php?pl1_id=40880.
7. Голицына, О. Л. Языки программирования [Электронный ресурс]: учебное пособие. — 2, перераб. и доп. — Москва: Издательство "ФОРУМ", 2010. — 400 с. — среднее профессиональное. — ISBN 978-5-91134-442-9. —
URL: <http://znanium.com/go.php?id=226043>.
8. Бабаш, А.В. Криптографические методы защиты информации [Электронный ресурс]: учебно-методическое пособие: том 1. 1. Криптографические методы защиты информации. — 2. — Москва; Москва: Издательский Центр РИОР: ООО "Научно-издательский центр ИНФРА-М", 2018. — 413 с. — ISBN 9785369012673. —
URL: <http://znanium.com/go.php?id=960001>.
9. Нестеров, С. А. Информационная безопасность [Электронный ресурс] : учебник и практикум / С. А. Нестеров. — Москва: Юрайт, 2018. — 321 с. — (Профессиональное образование). — Режим доступа: <https://www.biblio-online.ru>. — Internet access. — ISBN 978-5-534-07979-1. —
URL: <https://www.biblio-online.ru/bcode/424066>.
10. Огороков, В. А. Операционные системы [Текст]: курс лекций / В. А. Огороков. — Челябинск: Издательство Челябинского государственного университета, 2011. — 287 с.: ил. — (Классическое университетское образование). — Библиогр.: с. 283. — ISBN 978-5-7271-1055-3.
11. Гуцин, А. Н. Базы данных [Электронный ресурс]: учебник / А.Н. Гуцин. — Москва: Директ-Медиа, 2014. — 266 с.: ил.,табл., схем. —
<http://biblioclub.ru/>. — ISBN 978-5-4458-5147-9. —
URL: <http://biblioclub.ru/index.php?page=book&id=222149>. —
URL: <http://doi.org/10.23681/222149>.
12. Нужнов, Е. В. Компьютерные сети [Электронный ресурс]: учебное пособие. 2. Технологии локальных и глобальных сетей / Е.В. Нужнов;



Министерство образования и науки Российской Федерации; Южный федеральный университет; Инженерно-технологическая академия. — Таганрог: Издательство Южного федерального университета, 2015. — 176 с. : схем., табл., ил. — Библиогр. в кн. — <http://biblioclub.ru/>. — ISBN 978-5-9275-1691-9. — URL: <http://biblioclub.ru/index.php?page=book&id=461991>.

13. Хорев, П. Б. Программно-аппаратная защита информации [Электронный ресурс]: учебное пособие. — 2, испр. и доп. — Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. — 352 с. — ISBN 978-5-00091-004-7. — URL: <http://znanium.com/go.php?id=489084>.

Дополнительная литература

14. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. — 5-е изд., стер. — Москва: Академия, 2011. — 331 с.: ил. — (Высшее профессиональное образование, Информатика и вычислительная техника). — Библиогр.: с. 327-328. — ISBN 978-5-7695-7738-3.

15. Артемов, А. В. Информационная безопасность [Электронный ресурс]: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. — Орел: МАБИВ, 2014. — 257 с.: табл., схем. — <http://biblioclub.ru/>. — URL: <http://biblioclub.ru/index.php?page=book&id=428605>.

16. Дудецкий, В.Н. Объектно-ориентированные языки программирования [Электронный ресурс]: учебное пособие. — 2. — Москва: Издательство "Флинта", 2016. — 48 с. — ISBN 9785976522527. — URL: <http://znanium.com/go.php?id=1037567>.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

1. Лань [Электронный ресурс]: электронно-библиотечная система (ЭБС) / издательство Лань. — URL: <http://e.lanbook.com/>.

2. Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. — URL: <http://biblioclub.ru/>.

3. Юрайт [Электронный ресурс]: электронно-библиотечная система (ЭБС) / издательство Юрайт. — URL: <https://biblio-online.ru>.

4. Znanium.com [Электронный ресурс]: электронно-библиотечная система (ЭБС) / Научно-издательский центр ИНФРА-М. — URL: <http://znanium.com/>.



5. BOOK.ru [Электронный ресурс]: электронно-библиотечная система (ЭБС) / издательство КноРус. – URL: <https://www.book.ru/>.

6. eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. – URL: <http://elibrary.ru/defaultx.asp>.

7. ИНФОРМИО [Электронный ресурс]: электронный справочник [обеспечение всех типов образовательных учреждений нормативными, методическими, научно-практическими материалами]. – URL: <http://www.informio.ru/>.

7. Методические рекомендации студентам для подготовки к государственному экзамену

Студенту необходимо самостоятельно обобщить и систематизировать материал по дисциплинам:

- Математический анализ
- Теория вероятностей и математическая статистика
- Алгебра
- Теория информации
- Языки программирования
- Технологии и методы программирования
- Криптографические методы защиты информации
- Основы информационной безопасности
- Операционные системы
- Безопасность систем баз данных
- Безопасность сетей ЭВМ
- Программно-аппаратные средства обеспечения информационной безопасности

В ходе устного ответа комиссия может задать дополнительные вопросы по материалу всех дисциплин учебного плана.

При подготовке к экзамену студенту необходимо:

1. Проанализировать предложенную основную и дополнительную литературу, тексты лекций по дисциплинам, выносимым на государственный экзамен, и выбрать материал, который может составить содержание ответа;
2. Структурировать выбранный материал и подготовить план ответа на вопрос;
3. Проработать содержание каждого из пунктов плана, выбрать основные понятия и ключевые теоремы, подготовить их доказательство.



8. Материально-техническое обеспечение

Для подготовки и сдачи государственного экзамена имеется необходимая материально-техническая база, соответствующая действующим санитарным и противопожарным правилам и нормам, обеспечивающей проведение всех видов теоретической и практической подготовки:

– лекционные аудитории, оснащенные мультимедийными комплексами на основе антивандальной трибуны;

– специализированные компьютерные классы с подключенным к ним периферийным устройством и оборудованием.

Используются электронный читальный зал научной библиотеки ЧелГУ (аудитория 206) для самостоятельной работы студента, оснащенный персональными компьютерами, мультимедийной аппаратурой. В аудитории обеспечен доступ к различной справочной литературе, энциклопедиям, библиографическим и полнотекстовым базам данных, информационным ресурсам «Интернет».

Обучение инвалидов и лиц с ограниченными возможностями здоровья осуществляется с применением следующего специального оборудования:

а) для лиц с нарушением слуха (акустический усилитель¹ и колонки, мультимедийный проектор);

б) для лиц с нарушением зрения (мультимедийный проектор (использование презентаций с укрупненным текстом);

в) для лиц с нарушением опорно-двигательного аппарата (персональные мобильные компьютеры – нетбуки).

| Название кабинета | Оборудование |
|---|--|
| Тифлотехническая аудитория, кабинет А-28 первого учебного корпуса | Тифлотехнические средства: брайлевский компьютер с дисплеем и принтером, тифлокомплекс «Читающая машина», телевизионное увеличивающее устройство, тифломагнитолы кассетные (3 шт.) и цифровые диктофоны (6 шт.). Специальное программное обеспечение: программа речевой навигации JAWS, речевые синтезаторы («говорящая мышь»), экранные лупы. |
| Сурдотехническая аудитория, кабинет А-27 первого учебного корпуса | радиокласс «Сонет-Р» (на 6 человек), программируемые слуховые аппараты (6 шт.) индивидуального пользования с устройством задания режима работы на компьютере, аудиотехника. |
| Аудитория адаптивных информационных технологий, кабинет А-27 первого учебного корпуса | Компьютерный класс на 12 мест, интерактивная доска ActiveBoard с системой голосования, акустический усилитель и колонки, мультимедийный проектор, телевизор, видеомагнитофон, устройство видеоконференцсвязи VCON HD3000. |

¹ Акустический усилитель предоставляется РУНЦИО.