БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Ректор Белорусского
государственного университета
_____А.Д.Король
17 января 2025 г.
Регистрационный № 13672/гэ.

ПРОГРАММА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

для специальности

1-98 01 01 Компьютерная безопасность (по направлениям)

2025 г.

Программа государственного экзамена для специальности «1-98 01 01 Компьютерная безопасность (по направлениям)» разработана на основе образовательного стандарта высшего образования для специальности 1-98 01 01-2021; учебных программ по учебным дисциплинам: «Дифференциальное и интегральное исчисление» (от 02.07.2021 №УД-10201/уч.), «Функциональные последовательности и ряды, несобственный интеграл» (от 23.06.2022 № УД-10766/уч.), «Основы высшей алгебры» (от 02.07.2021 №УД-10158/уч.), «Аналитическая геометрия» (от 02.07.2021 №УД-10156/уч.), «Ряды и функции комплексного аргумента» (от 27.06.2022 №УД-10777/уч.), «Линейная алгебра» (от 08.10.2021 № УД-10157/уч.), «Основы и методологии программирования» (от 08.07.2022 № УД-11252/уч.), «Разработка кросс-платформенных приложений» (от 01.12.2022 №УД-11328/уч.), «Машинно ориентированное программирование» (от 1.12.2022 №УД-11329/уч.), «Промышленное программирование» (от 08.07.2022 №УД-11381/уч.), «Технологии программирования» (от 01.12.2022 № УД-11771/уч.), «Дискретная математика и математическая логика» (от 09.08.2021 № УД-10231/уч.), «Операционные системы» (от 05.07.2023, № УД-12474/уч.), «Модели данных и СУБД» (от 01.12.2022, УД-11600/уч.), «Дифференциальные уравнения» (от 08.07.2022 №УД-11477/уч.), «Функциональный анализ» (от 05.07.2023 № УД-12351/уч.), «Методы оптимизации» (от 12.06.2023 №УД-11863/уч.), «Численные методы» (от 05.06.2023 № УД-12598/уч.), «Криптографические методы» (от 30.06.2023 №УД-12735/уч.), «Теория информации» (от 05.07.2023 №УД-12599/уч.), «Компьютерные сети» (от 01.12.2023 №УД-12586/уч.).

СОСТАВИТЕЛИ:

В.И. Малюгин, заведующий кафедрой математического моделирования и анализа данных ФПМИ, доктор эконом. наук, кандидат физ.-мат. наук, профессор;
С.Н. Сталевская, доцент кафедры математического моделирования и анализа данных ФПМИ, кандидат физ.-мат. наук

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Советом факультета прикладной математики и нформатики БГУ (протокол № 4 от 24.12.2024);

Председатель Совета _____ Ю.Л.Орлович

Научно-методическим Советом БГУ (протокол № 6 от 16.01.2025)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Государственный экзамен является одной из обязательных составляющих итоговой аттестации студентов. Программа государственного экзамена по специальности 1-98 01 01 Компьютерная безопасность разработана в соответствии с требованиями государственного образовательного стандарта I ступени высшего образования и действующими Правилами проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования.

Программа государственного экзамена определяет и регламентирует структуру и содержание государственного экзамена по специальности 1-98 01 01 Компьютерная безопасность.

В программу государственного экзамена включаются следующие учебные дициплины и модули:

– учебные дисциплины «Дифференциальное и интегральное исчисление», «Функциональные последовательности и ряды, несобственный интеграл», «Ряды и функции комплексного аргумента», «Основы высшей алгебры», «Аналитическая геометрия», «Линейная алгебра» модуля «Высшая математика»,

– учебные дисциплины «Основы и методологии программирования», «Разработка кроссплатформенных приложений», «Промышленное программирование», «Техгологии программирования» модуля «Программирование»,

– учебная дисциплина «Дискретная математика и математическая логика» модуля «Дискретная математика и алгоритмы»,

– учебные дисциплины «Операционные системы», «Модели данных и СУБД» модуля «Информатика и компьютерные системы»,

– учебные дисциплины «Дифференциальные уравнения», «Функциональный анализ» модуля «Дифференциальные уравнения и функциональный анализ»,

– учебная дисциплина «Методы оптимизации» модуля «Математические методы принятия решений»,

– учебная дисциплина «Численные методы»,

– учебная дисциплина «Криптографические методы» модуля «Криптография»,

– учебные дисциплины «Теория информации», «Компьютерные сети» модуля «Информационно аналитические системы».

Государственный экзамен проводится на заседании государственной экзаменационной комиссии.

Цель проведения государственного экзамена по специальности – выявление компетенций специалиста, т. е. теоретических знаний и практических умений, необходимых для решения теоретических и практических задач специалиста с высшим образованием.

Программа государственного экзамена носит системный, междисциплинарный характер и ориентирована на выявление у выпускника общепрофессиональных и специальных знаний и умений. Выпускник должен:

знать:

– современный математический аппарат, применяемый при решении задач прикладной математики и информатики;

– основные задачи и области применения методов математического (численного, вероятностного) моделирования, численные характеристики и структурные особенности объектов моделирования, методики исследования моделей;

– методологические основы для проверки адекватности математических моделей, методы качественного и количественного анализа результатов математического моделирования;

– технологии программирования, методологии разработки программного обеспечения, методы и средства проверки работоспособности программного обеспечения, основные принципы отладки программного кода.

уметь:

– применять полученные знания математического аппарата для решения конкретных задач в области прикладной математики, информатики и кибербезопасности;

– применять методы математического моделирования к решению конкретных задач, строить и анализировать математические алгоритмы и реализовывать их с помощью языков программирования;

– применять информационные технологии в практической деятельности и анализировать полученные решения вычислительных задач.

владеть:

– навыками применения математического инструментария для создания и исследования новых математических моделей в области профессиональной деятельности, навыками построения и реализации основных математических алгоритмов;

– методами математического моделирования при анализе актуальных задач на основе глубоких знаний фундаментальных математических дисциплин и компьютерных наук.

Освоение образовательной программы 1-98 01 01 Компьютерная безопасность должно обеспечить формирование следующих компетенций:

универсальные компетенции:

УК. Владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации,

УК. Решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий,

базовые профессиональные компетенции:

БПК. Применять аппарат дифференциального и интегрального исчисления, методы аналитической геометрии и линейной алгебры для построения математических моделей и решения прикладных задач,

БПК. Строить, анализировать и тестировать алгоритмы и программы решения типовых задач обработки информации с использованием структурного, объектно-ориентированного и иных парадигм программирования,

БПК. Понимать предмет и объекты дискретной математики и математической логики, использовать основные приемы разработки эффективных алгоритмов и знания об основных структурах данных для решения прикладных задач,

БПК. Проектировать и разрабатывать реляционные базы данных средствами современных СУБД, применять знания в области принципов функционирования, архитектур и программных реализаций операционных систем для организации вычислительных процессов,

БПК. Использовать основные понятия и нормативную базу информационной безопасности для описания и классификации теоретических, правовых, организационных и инженерно-технических методов обеспечения конфиденциальности, целостности и доступности информации.

специализированные компетенции:

СК. Применять методы исследования и решения уравнений в частных производных в различных приложениях, интерпретировать полученные решения при исследовании естественно-научных процессов,

СК. Использовать методы функционального анализа и применять их для решения прикладных задач в различных областях науки, техники, экономики,

СК. Строить вероятностные модели в прикладных задачах, вычислять вероятности сложных случайных событий и исследовать важнейшие характеристики случайных величин, использовать методы математической статистики для решения задач оценивания параметров и проверки гипотез, применять методы анализа основных моделей случайных процессов,

СК. Использовать методы решения задач математического программирования, включая линейное, выпуклое, нелинейное, дискретное программирование, методы решения бесконечномерных задач оптимизации, применять теорию двойственности при исследовании оптимизационных задач,

СК. Использовать методы численного анализа для решения прикладных задач в различных сферах человеческой деятельности; применять навыки программной реализации вычислительных алгоритмов и анализа полученных результатов,

СК. Разрабатывать и анализировать надежность блочных и поточных криптосистем, функций хеширования, криптосистем с открытым ключом и систем электронной цифровой подписи,

СК. Понимать базовые принципы построения компьютерных систем и сетей, понимать и применять алгоритмы работы протоколов маршрутизации в IP-сетях, создавать сетевые приложения,

СК. Использовать базовые принципы построения и анализа математических моделей в типовых задачах организационного управления и естественно-интеллектуальной активности человека,

СК. Применять методы анализа и хранения больших объемов данных, осуществлять выбор подходящего инструмента анализа больших данных,

СК. Применять навыки проектирования и реализации систем безопасности, осуществлять выбор подходящего криптографического метода защиты типа данных и его реализации,

СК. Осуществлять статистический анализ данных с целью установления модели данных, выявлению кластерной структуры данных и аномальных наблюдений,

СК. Производить контроль целостности конфигурации операционной системы, создавать и производить настройку политик доступа и аудита операционных систем,

СК. Проводить статистический анализ дискретных данных с целью установления статистических зависимостей ,

СК. Выбирать и применять криптографические протоколы, обеспечивающие заданный уровень безопасности современных компьютерных систем.

ПОРЯДОК ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Экзамен (ответы студентов и беседа с экзаменующимися) проводится на русском или белорусском языке (указать другой язык).

В ходе подготовки, экзаменующиеся имеют право использовать учебные программы соответствующих дисциплин, научную и справочную литературу. Также в процессе подготовки может быть использован ***эвристический подход,*** который предполагает: осуществление студентами личностно-значимых открытий окружающего мира; демонстрацию многообразия решений большинства профессиональных задач и жизненных проблем; творческую самореализацию обучающихся в процессе создания образовательных продуктов; индивидуализацию обучения через возможность самостоятельно ставить цели, осуществлять рефлексию собственной образовательной деятельности.

На подготовку к ответу на государственном экзамене обучающемуся при освоении содержания образовательных программ высшего образования I ступени отводится не менее 30 минут не более одного астрономического часа, на сдачу государственного экзамена отводится до 30 минут.

СТРУКТУРА ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Вопросы экзаменационного билета по учебным модулям: «Высшая математика», Программирование», «Дискретная математика и алгоритмы», «Математические модели и методы в экономике», «Информатика и компьютерные системы», «Дифференциальные уравнения и функциональный

анализ», «Математические методы принятия решений», «Численные методы», «Криптография», «Информационно аналитические системы» - отражают содержание образовательной программы по специальности 1-98 01 01 Компьютерная безопасность.

Экзаменационный билет включает темы теоретического материала (два вопроса), позволяющие оценить полученные в процессе обучения знания.

Характеристика теоретической части:

Первый вопрос билета содержит разделы фундаментальных математических знаний, необходимых для решения прикладных задач, второй – знания из области копьютерной безопасности, а так же теории алгоритмов, программно-компьютерных технологий и алгоритмов.

Каждый экзаменационный вопрос затрагивает большой раздел или несколько разделов ранее изученных дисциплин. Отвечая на вопросы государственного экзамена, студент должен продемонстрировать грамотное изложение соответствующего материала, видение того, какое место и значение занимает этот материал в комплексе полученных знаний, междисциплинарные знания.

Для уточнения экзаменационной отметки члены ГЭК могут задавать обучающемуся дополнительные вопросы в соответствии с программой государственного экзамена. Количество дополнительных вопросов не должно превышать трех.

СОДЕРЖАНИЕ ПРОГРАММЫ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Раздел 1. Учебные дисциплины «Дифференциальное и интегральное исчисление», «Функциональные последовательности и ряды, несобственный интеграл», «Ряды и функции комплексного аргумента», «Основы высшей алгебры», «Аналитическая геометрия», «Линейная алгебра» модуля «Высшая математика»

Тема 1. Способы задания и исследования функций

Явное задание функций, их исследование методами дифференциального исчисления. Неявное задание функций. Функции, задаваемые как сумма ряда, как предел функциональной последовательности, как интегралы, зависящие от параметра.

Тема 2. Интеграл. Вычисление интегралов. Использование интегралов при моделировании и решении прикладных задач

Определение интеграла по Риману и Лебегу. Кратные, криволинейные и поверхностные интегралы. Вычисление интегралов. Несобственные интегралы. Примеры использования интегралов при решении технических, физических, экономических и др. задач.

Тема 3. Функциональные последовательности и ряды

Поточечная и равномерная сходимости функциональных последовательностей и рядов. Теорема о непрерывности суммы функционального ряда, теоремы о почленном дифференцировании и о почленном интегрировании функциональных рядов. Радиус сходимости степенного ряда и его вычисление. Представление функций степенными рядами и тригонометрическими рядами Фурье. Использование рядов при решении функциональных уравнений.

Тема 4. Ряды и функции комплексного переменного

Аналитическая функция. Особые точки. Вычисление вычетов в особых точках. Интегральная теорема Коши. Формула Коши для односвязных и многосвязных областей. Использование вычетов для вычисления интегралов.

Тема 5. Векторные пространства и линейные операторы в *конечномерных векторных пространствах*

Векторное пространство его базис и размерность. Линейные операторы в конечномерных векторных пространствах и их матрицы. Подобие матриц. Критерий подобия. Нормальные формы матриц.

Тема 6. Системы линейных алгебраических уравнений

Неоднородные системы. Критерий совместности линейных систем (теорема Кронекера-Капелли). Структура общего решения однородных и неоднородных систем.

Примерный перечень вопросов по разделу 1
для подготовки к государственному экзамену:

1. Функции одной и нескольких переменных
2. Интегралы
3. Функциональные последовательности и ряды
4. Функции комплексного переменного
5. Векторные пространства и линейные операторы в конечномерных векторных пространствах
6. Системы линейных алгебраических уравнений

Раздел 2. Учебная дисциплина «Дискретная математика и математическая логика» модуля «Дискретная математика и алгоритмы»

Тема 1. Основные комбинаторные конфигурации и их свойства

Перестановки, сочетания и размещения, формулы для подсчета их числа. Бином Ньютона и биномиальные коэффициенты. Мультимножества, сочетания с повторениями, их связь с сочетаниями без повторений.

Тема 2. Алгоритмически неразрешимые проблемы

Машина Тьюринга как формальная модель алгоритма. Понятие асимптотической временной сложности. Полиномиальные и экспоненциальные алгоритмы. Класс P. NP-полные задачи. Соотношения между классами.

Тема 3. Структуры данных. Базовые операции и их трудоемкость

Списки, стеки, очереди, кучи, система непересекающихся множеств. Базовые операции и их трудоемкость.

Тема 4. Организация поиска. Хеш-таблицы. Сбалансированные поисковые деревья. Базовые операции и их трудоемкость

Структуры данных для выполнения словарных операций. Хеш-таблицы. Методы разрешения коллизий. Бинарные поисковые деревья. Инварианты сбалансированности. АВЛ-дерево, поддержка инвариантов сбалансированности и их трудоемкость.

Тема 5. Базовые алгоритмы поиска на графах

Поиск в ширину и глубину в графе и их приложения (определение двудольности и связности графа, выделение сильно-связных компонент ориентировнаного графа). Топологическая сортировка вершин ориентированного графа. Алгоритмы построения минимального остовного дерева. Алгоритмы построения кратчайших маршрутов в графе.

Примерный перечень вопросов по разделу 2
для подготовки к государственному экзамену:

1. Основные комбинаторные конфигурации и их свойства.
2. Алгоритимически неразрешимые проблемы.

3. Простейшие структуры данных. Специализированные структуры данных.

4. Базовые операции и их трудоемкость. Выбор структуры данных для разработки эффективного алгоритма решения задачи.

5. Структуры данных для организации поиска элемента. Хеш-таблицы.

6. Сбалансированные поисковые деревья.

7. Базовые алгоритмы поиска на графах и их вычислительная сложность

Раздел 3. Учебные дисциплины «Дифференциальные уравнения», «Функциональный анализ» модуля «Дифференциальные уравнения и функциональный анализ»

Тема 1. Линейные дифференциальные уравнения и системы

Методы построения общих решений однородных и неоднородных уравнений и систем с постоянными коэффициентами, формула Коши для нестационарных линейных систем.

Тема 2. Общая теория дифференциальных уравнений

Существование и единственность решения задачи Коши (теорема Пикара-Линделефа). Непрерывная зависимость решений дифференциальных уравнений от начальных условий и правых частей. Устойчивость стационарных и нестационарных систем дифференциальных уравнений.

Тема 3. Принцип сжимающих отображений и его применение

Банахово пространство. Сжимающее отображение. Теорема Банаха о неподвижной точке сжимающего отображения. Применение принципа сжимающих отображений к решению СЛАУ и интегральных уравнений второго рода. Метод резольвент.

Тема 4. Компактные множества и компактные операторы

Компактные множества в конечномерных и бесконечномерных пространствах. Компактные операторы в банаховых пространствах. Компактность интегрального оператора. Разрешимость уравнений второго рода с компактным оператором. Теоремы Фредгольма.

Примерный перечень вопросов по разделу 3
для подготовки к комплексному государственному экзамену

1. Линейные дифференциальные уравнения и системы
2. Общая теория дифференциальных уравнений
3. Принцип сжимающих отображений и его применение
4. Компактные множества и компактные операторы

Раздел 4. Учебная дисциплина «Методы оптимизации» модуля «Математические методы принятия решений»

Тема 1. Симплекс-метод как основной метод решения задач линейного программирования

Постановка задачи линейного программирования. Графический метод решения. Геометрическая интерпретация итерации симплекс-метода. Базисный план. Потенциалы, оценки. Критерий оптимальности. Двойственная задача к канонической и нормальной формам. Физический смысл двойственных переменных.

Тема 2. Метод множителей Лагранжа в нелинейном и выпуклом программировании

Постановка задачи нелинейного программирования со смешанными ограничениями. Понятие регулярного плана. Функция Лагранжа (классическая). Классическое правило множителей Лагранжа. Выпуклые функции и множества. Задача выпуклого программирования. Седловая точка. Теорема Куна-Таккера. Условия Куна-Таккера в случае дифференцируемых функций.

Тема 3. Метод ветвей и границ, динамическое программирование для решения конечномерных экстремальных задач

Определение метода ветвей и границ. Схемы одностороннего и полного ветвлений. Примеры применения. Понятие динамического программирования. Три этапа решения. Задача распределения ресурсов (постановка, уравнение Беллмана, решение). Примеры применения метода динамического программирования.

Примерный перечень вопросов по разделу 4
для подготовки к комплексному государственному экзамену

1. Симплекс-метод как основной метод решения задач линейного программирования
2. Метод множителей Лагранжа в нелинейном и выпуклом программировании
3. Метод ветвей и границ, динамическое программирование для решения конечномерных экстремальных задач

Раздел 5. Учебная дисциплина «Численные методы»

Тема 1. Численные методы решения нелинейных уравнений, систем и задач оптимизации

Итерационные методы решения нелинейных уравнений и систем: метод простой итерации, Ньютона и его видоизменения. Градиентные методы и метод Ньютона для решения задач нелинейной оптимизации.

Тема 2. Приближение функций. Основные способы приближения функций и соответствующие алгоритмы

Существование и единственность элемента наилучшего приближения в линейных нормированных пространства. Наилучшее среднеквадратичное

приближение. Интерполирование: основные представления интерполяционного многочлена и остатка интерполирования. Сплайн-приближения.

Тема 3. Приближенное вычисление интегралов

Основные типы квадратурных формул (интерполяционные квадратуры, квадратуры наивысшей алгебраической степени точности); практическая оценка погрешности квадратур. Простейшие кубатурные формулы.

Тема 4. Методы численного решения начальных и граничных задач для обыкновенных дифференциальных уравнений

Одношаговые (Рунге-Кутта) и многошаговые (Адамса) методы решения начальной задачи, их простейшие характеристики; правило Рунге практической оценки погрешности; методы решения граничных задач: основанные на сведении к начальной задаче, проекционные, сеточные.

Примерный перечень вопросов по разделу 5
для подготовки к комплексному государственному экзамену

1. Численные методы решения нелинейных уравнений, систем и задач оптимизации
2. Приближение функций. Основные способы приближения функций и соответствующие алгоритмы
3. Приближенное вычисление интегралов
4. Методы численного решения начальных и граничных задач для обыкновенных дифференциальных уравнений

Раздел 6. Учебные дисциплины «Основы и методологии программирования», «Разработка кроссплатформенных приложений», «Промышленное программирование», «Техгологии программирования» модуля «Программирование»

Тема 1. Основные типы данных в языках программирования и операции над ними

Определение типа. Базовые типы данных и их характеристики. Структурированные типы. Построение пользовательских типов данных на основе базовых типов.

Тема 2. Модульное программирование

Функции. Объявление и определение функции. Формальные и фактические параметры. Способы передачи параметров. Рекурсивные функции. Перегрузка функций. Указатели на функцию. Передача функции в качестве параметра. Встроенные функции. Шаблоны функций.

Тема 3. Основы объектно-ориентированного программирования

Класс как абстрактный тип, классы и объекты. Члены класса, управление доступом. Конструкторы, деструкторы. Перегрузка операторов.

Тема 4. Наследование и полиморфизм как базовые понятия в парадигме объектно-ориентированного программирования

Основные принципы и правила наследования. Понятие производного класса. Базовый класс и атрибуты его доступа. Иерархия производных классов. Конструкторы производных классов. Основные принципы и правила полиморфизма. Виртуальные функции. Виртуальные деструкторы. Указатели объектов производного и базовых классов. Статическое и динамическое связывание.

Тема 5. Реализация концепций ООП в различных языках программирования

Создание класса. Доступ к элементам класса. Спецификаторы доступа. Инкапсуляция и полиморфизм в языках C++ и Java.

Тема 6. Паттерны проектирования

Понятие паттерна проектирования Классификация паттернов объектно-ориентированного проектирования. Порождающие паттерны. Структурные паттерны. Паттерны поведения. Методология решения задач проектирования с помощью паттернов. Технология использования паттерна.

Тема 7. Кроссплатформенное программирование

Определение кроссплатформенности. Уровни кроссплатформенности: аппаратный, программный, компиляции, выполнения. Проблемы кроссплатформенной разработки. Реализация кроссплатформенности на уровне компиляции и на уровне выполнения. Кроссплатформенные среды разработки. Подходы к кроссплатформенному программированию. Кроссплатформенный пользовательский интерфейс и проблемы его создания.

Тема 8. Управление кодом и документирование проекта в продуктовой разработке

Системы контроля версий (СКВ) для управления исходным кодом приложений. Типы СКВ. Распределенная система контроля версий и управления кодом git. Установка git. Создание и инициализация репозитория. Клонирование репозитория. Состояния файлов под управлением git. Запись и фиксация изменений в локальный репозитории. Внешние репозитории, подключение и настройка. Публикация изменений во внешний репозиторий и получение изменений из репозитория. Управление локальными и внешними ветками. Консольный клиент git. Графические клиентские приложения управления версиями. Язык разметки Markdown. Документирование проекта с помощью файла README. Документирование проекта в wiki. Github Pages и другие сервисы документирования проектов.

Тема 9. Принципы дизайна и парадигмы программирования

Ограничения, связанные с парадигмой программирования. Структурное программирование. Объектно-ориентированное программирование. Функциональное программирование. Принцип единственной ответственности — Single Responsibility Principle (SRP). Принцип открытости / закрытости — Open-Closed Principle (OCP). Принцип подстановки Барбары Лисков — Liskov Substitution Principle (LSP). Принцип разделения интерфейсов — Interface Segregation Principle (ISP). Принцип инверсии зависимости — Dependency Inversion Principle (DIP).

Тема 10. Жизненный цикл программного продукта

Различные модели жизненного цикла программного продукта (каскадная модель, спиральная модель, V-образная модель, инкрементная (пошаговая) модель, модель быстрого прототипирования). Модели промышленных технологий создания программного продукта (Модель Microsoft Solution Framework (MSF), Agile-методологии, Модель Rational Unified Process (RUP), Модель Extreme Programming (XP)). Тестирование и отладка программного обеспечения.

Примерный перечень вопросов по разделу 6
для подготовки к государственному экзамену:

1. Основные типы данных в языках программирования и операции над ними.
2. Функции. Способы передачи параметров. Рекурсивные и встроенные функции. Перегрузка функций. Шаблоны функций.
3. Класс как абстрактный тип, классы и объекты. Члены класса, управление доступом. Конструкторы, деструкторы. Перегрузка операторов.
4. Наследование и полиморфизм как базовые понятия в парадигме объектно-ориентированного программирования.
5. Реализация концепций ООП в различных языках программирования.
6. Паттерны проектирования. Классификация паттернов объектно-ориентированного проектирования. Технология использования паттерна.
7. Кроссплатформенное программирование. Определение. Уровни кроссплатформенности. Проблемы кроссплатформенной разработки.
8. Кроссплатформенные среды разработки.
9. Системы контроля версий для управления исходным кодом приложений. Распределенная система контроля версий и управления кодом git.
10. Принципы дизайна и парадигмы программирования.
11. Модели жизненного цикла программного обеспечения.
12. Тестирование программного обеспечения.

Раздел 7. Учебные дисциплины «Операционные системы», «Модели данных и СУБД» модуля «Информатика и компьютерные системы»

Тема 1. Процессы и потоки

Определения. Состояния потока. Диаграмма состояний потока. Планирование процессов в операционных системах. Алгоритмы планирования процессов: FCFS, SPN, RR, SRT.

Тема 2. Взаимодействие процессов

Синхронизация потоков. Условная синхронизация, взаимное исключение. Каналы передачи данных. Передача сообщений между процессами, типы адресации процессов. Синхронный и асинхронный обмен данными.

Тема 3. Определение понятий «базы данных» и «СУБД»

Классификация СУБД по типам поддерживаемых моделей. Клиент-серверные и настольные СУБД. Фазы жизненного цикла системы обработки данных.

Тема 4. Проектирование БД. Реляционная модель базы данных. Нормализация данных, типы нормальных форм

Ключи, требования к ключам. Функциональные зависимости. Нормализация данных, типы нормальных форм.

Тема 5. Язык SQL

Составные части SQL: язык определения данных (DDL), язык манипуляции данными (DML). Понятие транзакции, операторы управления транзакциями.

Примерный перечень вопросов по разделу 7
для подготовки к государственному экзамену:

1. Процессы и потоки
2. Взаимодействие процессов
3. Процессы и потоки
4. Взаимодействие процессов
5. Язык SQL

Раздел 8. Учебная дисциплина «Криптографические методы» модуля «Криптография»

Тема 1. Блочные криптосистемы

Блочно-итерационные криптосистемы. Схема подстановки-перестановки. Криптосистема AES. Использование инволютивных подстановок. Схема Фейстеля. Криптосистемы Фейстеля: DES, ГОСТ 28147. Условия атак. Задачи криптоанализа. Сложность атак. Основные методы криптоанализа. Режимы шифрования. Имитозащита.

Тема 2. Поточные криптосистемы

Поточные криптосистемы как конечные автоматы. Регистры сдвига с линейной обратной связью. Свойства линейных рекуррентных последовательностей. Постулаты Голомба. Комбинирование регистров сдвига с линейной обратной связью: комбинирующий генератор, фильтрующий генератор, сжимающий и самосжимающий генераторы. Криптосистема A5/1.

Тема 3. Функции хэширования

Определения и задачи криптоанализа. Применение функций хэширования. Блочно-итерационные функции хэширования. Функции хэширования на основе блочных криптосистем. Атака «дней рождения». Ключезависимые функции хэширования.

Тема 4. Криптосистемы с открытым ключом

Функции с лазейкой. Использование функций с лазейкой для построения криптосистем с открытым ключом. Криптосистема RSA. Реализация RSA:

арифметика больших чисел, генерация простых, оптимизация. Задача факторизации. Методы факторизации: ρ-метод, метод p – 1, квадратичное решето.

Тема 5. Электронная цифровая подпись

Схема Эль-Гамаля. Схема Шнорра. Система ЭЦП СТБ 1176.2. Задача дискретного логарифмирования. Методы логарифмирования: метод «больших – малых шагов», ρ-метод, метод Поллига – Хеллмана.

Примерный перечень вопросов по разделу 8
для подготовки к государственному экзамену:

1. Блочно-итерационные криптосистемы.
2. Поточные криптосистемы.
3. Функции хэширования
4. Криптосистемы с открытым ключом
5. Электронная цифровая подпись

Раздел 9. Учебные дисциплины «Теория информации», «Компьютерные сети» модуля «Информационно аналитические системы»

Тема 1. Энтропия и количество информации по Шеннону, их свойства

Функционал энтропии и его свойства. Условная энтропия и ее свойства. Удельная энтропия стационарной символьной последовательности. Оптимизация функционала дифференциальной энтропии на классе вероятностных распределений. Количество информации по Шеннону и его свойства.

Тема 2. Теоретическая и практическая стойкость шифров по Шеннону

Шенноновские модели криптосистем. Элементарные криптосистемы. Теоретико-информационные оценки стойкости симметричных криптосистем. Совершенная криптостойкость. Пессимистическое утверждение Шеннона. Расстояние единственности

Тема 3. Модели, протоколы, технические средства построения компьютерных сетей

Сетевые модели. Базовые технологии локальных сетей (краткая характеристика технологий Ethernet, TokenRing, FDDI). IP-сети. Коммутация и маршрутизация. Протоколы прикладного уровня.

Тема 4. Системы и сети передачи информации

Модель взаимосвязи открытых систем (модель OSI/ISO) как основа построения систем связи. Основы передачи данных. Концептуальное описание основных сетей передачи данных: телефонной сети общего пользования, сети передачи данных, корпоративные сети, сети следующего поколения.

Примерный перечень вопросов по разделу 9

для подготовки к государственному экзамену:

1. Энтропия и количество информации по Шеннону
2. Теоретическая и практическая стойкость шифров по Шеннону.
3. Модели, протоколы, технические средства построения компьютерных сетей
4. Системы и сети передачи информации

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Волк, В. К. Базы данных. Проектирование, программирование, управление и администрирование : учебник для вузов / В. К. Волк. - 3-е изд., стер. - Санкт-Петербург: Лань, 2022. - 244 с.
2. Горлач, Б. А. Математическое моделирование. Построение моделей и численная реализация : учебное пособие для студентов вузов, / Б. А. Горлач, В.Г. Шахов. - Изд. 5-е, стер. - Санкт-Петербург; Москва; Краснодар: Лань, 2023. - 291с.
3. Гороховик, В. В. Математические основы теории потребления : учебное пособие для студентов учреждений высшего образования по специальности "Математика (по направлениям)" / В. В. Гороховик ; БГУ. - Минск : БГУ, 2021. - 127 с.
4. Заздравных, А. В. Экономика отраслевых рынков : учебник и практикум для вузов, для студ., обуч. по экон. спец. / А. В. Заздравных, Е. Ю. Бойцова. - 2-изд. - Москва : Юрайт, 2023. - 359 с.
5. Котов, В. М. Теория алгоритмов. Организация перебора и приближенные алгоритмы: учеб. -метод. пособие / В. М. Котов, Е. П. Соболевская, Г. П. Волчкова. – Минск: БГУ, 2022. – 151 с.
6. Курош А. Г. Курс высшей алгебры: учебник для вузов / Курош А. Г. - 25-е изд., стер. - Санкт-Петербург : Лань, 2024. - 432 с.
7. Лафоре, Р. Объектно-ориентированное программирование в C++ / Р. Лафоре ; [пер. с англ.: А. Кузнецов, М. Назаров, В. Шрага]. – 4-е изд – Санкт-Петербург ; Москва ; Минск : Питер, 2022. – 923 с.
8. Лафоре, Р. Структуры данных и алгоритмы Java / Роберт Лафоре ; [пер. с англ. Е. Матвеев]. - 2-е изд. - Санкт-Петербург; Москва; Минск: Питер, 2023. - 701с.
9. Мазалов, В. В. Математическая теория игр и приложения: учебное пособие [для вузов] / В. В. Мазалов. - Изд. 6-е, стер. - Санкт-Петербург; Москва; Краснодар: Лань, 2024. - 496 с. . Марчук, Г.И. Методы вычислительной математики: учебное пособие / Г.И. Марчук. – 4-е изд., стер. – Санкт-Петербург: Лань, 2022. – 608 с.
10. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / Виктор Олифер, Наталья Олифер - Санкт-Петербург [и др.] : Питер, 2020.
11. Размыслович, Г. П. Аналитическая геометрия: учебные материалы для студентов факультета прикладной математики и информатики. В 2 ч. Ч.1. истемы координат. Векторы / Г. П. Размыслович, А. В. Филипцов. - Минск : БГУ, 2022.
12. Размыслович, Г. П. Аналитическая геометрия: учебные материалы для студентов факультета прикладной математики и информатики. В 2 ч. Ч.2.

Линии и поверхности первого и второго порядков / Г. П. Размыслович, А. В. Филипцов. - Минск : БГУ, 2022. - 57с.

13. Сборник задач по теории алгоритмов. Структуры данных: учеб.-метод. пособие / С. А. Соболь [и др.] – Минск: БГУ, 2020. – 159 с.

14. Чеб, Е. С. Интегральные преобразования : учеб. материалы для студ. фак. прикладной математики и информатики : в 2 ч. / Е. С. Чеб ; БГУ, Фак. Прикладной математики и информатики, Каф. компьютерных технологий и систем. – Минск : БГУ, - Ч. 2 : . - 2022. - 61 с.

Дополнительная литература

15. Амосов, А. А. Вычислительные методы: Учебное пособие / А. А. Амосов, Ю. А. Дубинский, Н. В. Копченова. – СПб.: Издательство «Лань», 2014. –672 с.

16. Асанов, М. О. Дискретная математика: графы, матроиды, алгоритмы. Учебное пособие / М. О. Асанов, В. А. Баранский, В. В. Расин. – Спб.: Лань,

17. 2010. – 368 с.

18. Ахо, А. В. Структуры данных и алгоритмы / А. В. Ахо, Д. Э. Хопкрофт, Д. Д. Ульман.– М.: Вильямс, 2016. – 400 с.

19. Богданов, Ю. С. Лекции по математическому анализу/ Ю. С. Богданов. – Мн.: изд-во БГУ, 1974, 1978.– Ч. 1-2.

20. Богданов, Ю. С. Математический анализ / Ю. С. Богданов, О. А. Кастрица, Ю. Б. Сыроид.– М.: ЮНИТИ-ДАНА, 2003. – 351 с.

21. Богданов, Ю. С. Дифференциальные уравнения / Ю. С. Богданов, Ю. Б. Сыроид. –Мн.: Выш. школа, 1983. – 239 с.

22. Богданов, Ю. С. Курс дифференциальных уравнений / Ю. С. Богданов, С. А. Мазаник, Ю. Б. Сыроид. – Мн.: Университетское, 1996. – 287 с

23. Вагнер, Г. Основы исследования операций: в 3-х томах / Г. Вагнер. – М.: Мир, 1972-73. –335 с., – 487 с., – 501 с.

24. Введение в теоретико-числовые методы криптографии: учебное пособие для вузов / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург: Лань, 2024. — 396 с. — ISBN 978-5-507-47610-7. - URL: https://e.lanbook.com/book/397286

25. Вентцель, Е. С. Исследование операций: задачи, принципы, методология : учебное пособие / Е. С. Вентцель. – М.: КНОРУС, 2013. – 192 с.

26. Дейт, К. Дж. Введение в системы баз данных, 8-е изд. / К. Дж. Дейт. – М.: Издательский дом «Вильяме», 2005. – 1328 с.

27. Демидович, Б. П. Сборник задач и упражнений по математическому анализу: Учебное пособие – 20-е изд., стер. / Б. П. Демидович. – СПб.: Издательство «Лань», 2018 – 624 с.

28. Зорич, В. А. Математический анализ. – М.: Наука, 1997, 1998. – Ч. 1-2.

29. Зуев, Ю. А. По океану дискретной математики: от перечислительной комбинаторики до современной криптографии. Т. 1: Основные структуры. Методы перечисления. Булевы функции / Ю. А. Зуев. – М.: Книжный дом
30. «ЛИБРОКОМ», 2012. – 274 с.
31. Зуев, Ю. А. По океану дискретной математики: от перечислительной комбинаторики до современной криптографии. Т. 2: Графы. Алгоритмы. Коды, блок-схемы, шифры / Ю. А. Зуев. – М.:Книжный дом «ЛИБРОКОМ», 2012. – 368 с.
32. Игошин, В. И. Теория алгоритмов: учеб. пособие для студ. высш. учеб. заведений / В. И. Игошин. – М.: ИНФРА-М, 2012. – 318 с.
33. Игошин, В. И. Математическая логика. Учебное пособие / В. И. Игошин. – М.: Инфра-М, 2016. – 400 с.
34. Коберн, А. Быстрая разработка программного обеспечения / А. Коберн– М.: ЛОРИ, 2013. –314 с.
35. Компиляторы: принципы, технологии и инструментарий / А. Ахо [идр.]. –М.: Вильямс, 2018. – 1184 с.
36. Котов, В. М. Алгоритмы и структуры данных: учеб. пособие /В. М. Котов, Е. П. Соболевская, А. А. Толстиков – Минск: БГУ, 2011. – 267 с.
37. Корзюк, В. И. Уравнения математической физики / В. И. Корзюк. – Минск: «Издательский центр БГУ», 2011. –460 с.
38. Краснопрошин, В. В. Исследование операций: уч. пособие / В. В. Краснопрошин, Н. А. Лепешинский – Мн.: БГУ, 2013. – 191 с.
39. Криптология: учебник для студентов учреждений высшего образования по математическим и техническим специальностям / [Ю. С. Харин и др.]; БГУ. – 2-е изд., пересмотр. – Минск: БГУ, 2023. – 511 с. – URL: https://elib.bsu.by/handle/123456789/309839.
40. Крылов, В. И. Вычислительные методы высшей математики /В. И. Крылов, В. В. Бобков, П. И. Монастырный. – Мн.: Выш. школа, 1972.– 594 с
41. Кудрявцев, Л. Д. Курс математического анализа. – М.: Высш. шк., 1988, 1988, 1989. – Т. 1-3.
42. Куроуз, Д., Росс, К. Компьютерные сети: нисходящий подход / Д. Куроуз, К. Росс. – М.:Эксмо, 2016. 912 с
43. Лекции по теории графов: учебное пособие / В. А. Емеличев [и др.]. – М.: Либроком, 2015. – 390 с.
44. Макконнелл, С. Совершенный код. Мастер-класс / Пер. с англ. – М.:Издательство «Русская редакция», 2010. – 896 с.
45. Максимов, Н. В. Архитектура ЭВМ и вычислительных систем /Н. В.Максимов, Т. Л. Партыка, И. И Попов. – М.: ФОРУМ, 2012 – 512 с.
46. Методы оптимизации: Учебное пособие / Р. Габасов [и др.]. – Минск: Издательство «Четыре четверти», 2011. – 472 с.
47. Милованов, М. В.Алгебра и аналитическая геометрия, Часть 1 /М. В.Милованов, Р. И. Тышкевич, А. С. Феденко.– Мн.: Выш. шк., 1984. – 302 с.
48. Милованов, М. В.Алгебра и аналитическая геометрия, Часть 2 /М. В. Милованов, Р. И. Тышкевич, А. С. Феденко.– Мн.: Выш. шк., 1987. – 269 с.

49. Пападимитриу, Х. Комбинаторная оптимизация: Алгоритмы и сложность / Х. Пападимитриу, К. Стайглиц. – М.: Мир, 1971. – 512 с.

50. Приемы объектно-ориентированного проектирования. Паттерны проектирования/ Э. Гамма [и др.]. –СПб.: Питер, 2015. – 368 с.

51. Размыслович, Г. П. Геометрия и алгебра / Г. П. Размыслович, М. М. Феденя, В. М. Ширяев. – Мн.: Университетское, 1987.– 350 с.

52. Размыслович, Г. П. Сборник задач по геометрии и алгебре / Г. П. Размыслович, М. М. Феденя, В. М. Ширяев. – Мн.: Университетское, 1999.– 384с.

53. Рассел, С. Искусственный интеллект: современный подход / С. Рассел, П. Норвиг. – М.: Издательский дом «Вильямс», 2007.–1424 с.

54. Рейнгольд, Э. Комбинаторные алгоритмы теория и практика/ Э. Рейнгольд, Ю. Нивергельт, Н. Део. –М.: Мир, 1980. – 476 с.

55. Ржевский, С. В. Исследование операций: Учебное пособие /С. В. Ржевский. – СПб.: Издательство «Лань», 2013. – 480 с.

56. Сборник задач по теории алгоритмов : учеб.-метод. пособие / В.М. Котов, Ю.Л. Орлович, Е.П. Соболевская, С.А. Соболь – Минск : БГУ, 2017.- 183с

57. Сидоров, Ю. В. Лекции по теории функций комплексного переменного / Ю. В. Сидоров, М. В. Федорюк, М. И. Шабунин. – М.: Наука, 1989. – 408 с.

58. Скиена, С. Алгоритмы. Руководство по разработке / С. Скиена. – Издательство БХВ-Петербург, 2021. – 720 с.

59. Таха, Х. А. Введение в исследование операций / Х. А. Таха. – М.: Издательский дом «Вильямс», 2001. – 912 с.

60. Теория алгоритмов: учеб. пособие / П. А. Иржавский [и др.]. – Минск: БГУ, 2013. – 159 с.

61. Тер-Крикоров, А.М. Курс математического анализа / А. М. Тер-Крикоров, М. И. Шабунин. – М.: Наука, 1997. – 720 с.

62. Функции комплексного переменного. Операционное исчисление. Теория устойчивости / М. Л. Краснов [и др.]. – М.: Наука, 1981. – 303 с.

63. Харари, Ф. Теория графов / Ф. Харари. – М.: Ленанд, 2018. – 304 с.

64. Харин*, Ю.С.* Математическая и прикладная статистика / Ю. С. Харин, Е. Е. Жук – Мн.: БГУ, 2005. – 279 с.

65. Харин*, Ю.С.* Теория вероятностей / Ю. С. Харин, Н. М. Зуев – Мн.: БГУ, 2004. – 199 с.

66. Хопкрофт, Дж. Э. Введение в теорию автоматов, языков и вычислений / Дж. Э. Хопкрофт, Р. Мотвани, Дж. Ульман. – М.: Вильямс, 2008. – 528 с.

67. Шагин, В. Л. Теория игр: учебник и практикум для академического бакалавриата / В. Л. Шагин. – М.: Издательство Юрайт, 2015. – 223 с.

68. Ширяев, А. Н. Вероятность. В 2-х кн./ А. Н. Ширяев. – М.: МЦНМО, 2004. – 928 с.

69. Яблонский, С. В. Введение в дискретную математику / С. В. Яблонский. – М.: Высшая школа, 2003. – 384 с.

ЭУМК

70. Алгоритмы и структуры данных : электронный учебно-методический комплекс для специальностей 6-05-0533-09 «Прикладная математика», 6-05-0533-10 «Информатика», 6-05-0533-11 «Прикладная информатика», 6-05-0533-«Кибербезопасность». В 3 ч. Ч. 2 / Е.П. Соболевская, В.М. Котов, А.А. Буславский ; БГУ, Фак. прикладной математики и информатики, Каф. дискретной математики и алгоритмики. – Минск : БГУ, 2025. – 153 с. : ил. –Библиогр.: с. 147–148. https://elib.bsu.by/handle/123456789/324674

71. Дифференциальные уравнения в частных производных и их приложения : электронный учебно-методический комплекс для специальности: 1-31 03 04 «Информатика» / И. С. Козловская ; БГУ, Фак. прикладной математики и информатики, Каф. компьютерных технологий и систем. – Минск: БГУ, 2023. – 149 с. : ил. – Библиогр.: с. 148–149. https://elib.bsu.by/handle/123456789/304443

72. Сборник задач по теории алгоритмов. Организация перебора и приближенные алгоритмы : электронный учебно-методический комплекс для специальности: 1-31 03 04 «Информатика» / В. М. Котов, Е. П. Соболевская, Г.П. Волчкова ; БГУ, Фак. прикладной математики и информатики, Каф. дискретной математики и алгоритмики. – Минск : БГУ, 2021. – 144 с. : ил. –Библиогр.: с. 143–144. https://elib.bsu.by/handle/123456789/272717

73. Математический анализ : электронный учебно-методический комплекс для специальности: 1-31 03 04 «Информатика». В 3 ч. Ч. 3 / С. А. Мазаник, О. А. Кастрица ; БГУ, Фак. прикладной математики и информатики, Каф. высшей математики. – Минск : БГУ, 2021. – 105 с. : ил. − Библиогр.: с. 94–97. https://elib.bsu.by/handle/123456789/257817

74. Математический анализ : электронный учебно-методический комплекс для специальности: 1-31 03 04 «Информатика». В 3 ч. Ч. 1 / С. А. Мазаник, О. А.Кастрица ; БГУ, Фак. прикладной математики и информатики, Каф. высшей математики. – Минск : БГУ, 2020. – 75 с. − Библиогр.: с. 67–69. https://elib.bsu.by/handle/123456789/244693

75. Методы оптимизации : электронный учебно-методический комплекс для специальностей: 1-31 03 03 «Прикладная математика (по направлениям)»; 1-31 03 04 «Информатика»; 1-31 03 05 «Актуарная математика»; 1-31 03 06-01 «Экономическая кибернетика (по направлениям)», 1-98 01 01-01 «Компьютерная безопасность (по направлениям)» / В. В. Альсевич [и др.] ; БГУ, Фак. прикладной математики и информатики, Каф. методов оптимального управления. – Минск : БГУ, 2020. – 203 с. : ил., табл. – Библиогр.: с. 202–203 https://elib.bsu.by/handle/123456789/243989

76. Геометрия и алгебра : электронный учебно-методический комплекс для специальностей: 1-31 03 03 «Прикладная математика (по направлениям)», 1-31 03 04 «Информатика», 1-31 03 05 «Актуарная математика», 1-31 03 06-01 «Экономическая кибернетика (по направлениям)», 1-98 01 01-01 «Компьютерная безопасность (по направлениям)» / БГУ, Фак. прикладной математики и

информатики, Каф. высшей математики ; сост.: Г. П. Размыслович, А. В. Филипцов. – Минск : БГУ, 2020. – 2803 с. : ил. – Библиогр.: с. 2802–2803. http://elib.bsu.by/handle/123456789/242860