

Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе
и образовательным инновациям



О.И.Чуприс

17.01 2018 г.

Регистрационный № 4699

**Государственный экзамен
по специальности, направлению специальности, специализации**

Учебная программа учреждения высшего образования

для специальности:

1-98 01 01 Компьютерная безопасность (по направлениям)

направление специальности:

1-98 01 01- 01 Компьютерная безопасность (математические методы
и программные системы)

специализации:

1-98 01 01 01 01 Математические методы защиты информации

1-98 01 01 01 03 Защищенные информационные системы

2018 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-98 01 01- 2013 и учебного плана №Р98-138/уч. от 30.05.2013.

СОСТАВИТЕЛИ:

Агиевич Сергей Валерьевич, доцент кафедры математического моделирования и анализа данных, кандидат физико-математических наук;

Бодягин Игорь Александрович, доцент кафедры математического моделирования и анализа данных, кандидат физико-математических наук;

Харин Юрий Семенович, заведующий кафедрой математического моделирования и анализа данных, доктор физико-математических наук, член-корреспондент НАН Беларуси.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Советом факультета прикладной математики и информатики БГУ, протокол №2 от 24.10.2017г.;

Научно-методическим советом БГУ, протокол №2 от 15.11.2017г.



ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Государственный экзамен является одной из форм итоговой аттестации на первой ступени высшего образования. Наряду с подготовкой и защитой дипломного проекта служит для определения соответствия результатов учебной деятельности обучающихся требованиям образовательного стандарта, учебно-программной документации образовательной программы высшего образования при завершении обучения.

Программа и порядок проведения государственного экзамена разработаны в соответствии с Правилами проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования, утвержденными Постановлением Министерства образования Республики Беларусь 29.05.2012 № 53.

Цели государственного экзамена:

- комплексная оценка уровня теоретической и практической подготовки выпускника к выполнению социально-профессиональных задач, и установление соответствия его подготовки требованиям образовательного стандарта ОСВО 1-98 01 01-2013;
- решение вопроса о присвоении выпускнику соответствующей квалификации и выдаче ему диплома о высшем образовании (с учетом результатов защиты дипломной работы);
- определение путей дальнейшего совершенствования подготовки выпускников.

Итоговый государственный экзамен носит комплексный характер, т.е. ориентирован на выявление целостной системы общепрофессиональных и специальных научных знаний в области компьютерной безопасности. Программа государственного экзамена разработана на основе типовых учебных программ по учебным дисциплинам, а также учебным программам учреждения высшего образования. Его содержание формируется на междисциплинарной основе и включает три основных раздела:

I. Математические основы защиты информации.

II. Компьютерные основы защиты информации.

III. Специальные вопросы защиты информации.

В ходе проведения государственного экзамена проверке подлежат академические и профессиональные компетенции выпускника, его способность использовать на практике интегральную (междисциплинарную) методологию, умение обоснованно анализировать содержание (научные факты, теории, методы и т.п.) учебных дисциплин и использовать их в качестве средства для выполнения профессиональной деятельности.

На основе содержания программы государственного экзамена разрабатываются экзаменационные материалы, которые представляют собой перечень вопросов для проверки готовности выпускников к выполнению различных видов профессиональной деятельности.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

I. МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Способы задания функций и их исследование методами дифференциального исчисления.

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.

2. Типы интегралов, их использование в анализе и приложениях.

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. Простейшие квадратурные формулы.

3. Функциональные последовательности и ряды, их использование в анализе и приложениях.

Сходимость рядов и последовательностей. Представление функций степенными рядами и тригонометрическими рядами Фурье. Ряды Фурье в гильбертовых пространствах, полные ортонормированные системы функций. Использование рядов при решении дифференциальных и интегральных уравнений.

4. Аналитические функции и их особые точки. Вычеты. Интегральная теорема Коши.

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

5. Системы линейных алгебраических уравнений. Структура множества решений. Аналитические и численные методы решения систем.

Неоднородные системы. Критерий совместности линейных систем (теорема Кронекера-Капелли). Структура общего решения однородных и неоднородных систем. Обусловленность линейных систем. Основные прямые и итерационные методы решения систем.

6. 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.

7. Линейные дифференциальные уравнения и системы с постоянными коэффициентами.

Общее решение линейных однородных уравнений и систем. Структура решения неоднородных уравнений и систем, методы интегрирования. Задача Коши для линейных уравнений и систем.

8. Существование и единственность решения задачи Коши для обыкновенных дифференциальных уравнений. Методы численного решения начальных задач

Постановка задачи Коши для обыкновенных дифференциальных уравнений n -го порядка. Существование и единственность решения задачи Коши для дифференциальных уравнений (теорема Пикара-Линделефа). Основные методы численного решения начальных задач. Практическая оценка погрешности численного решения.

9. Банаховы пространства. Принцип сжимающих отображений и его приложения.

Банаховы пространства. Примеры. Пространство $C[a,b]$, $L_p[a,b]$. Сжимающие отображения в банаховых пространствах. Теорема Банаха. Применение принципа сжимающих отображений к решению алгебраических уравнений и интегральных уравнений второго рода.

10. Понятие о вероятности. Случайные величины, их распределения вероятностей и числовые характеристики.

Простейшие вероятностные модели: классическая, дискретная, геометрическая. Аксиомы Колмогорова. Формулы полной вероятности и Байеса. Понятие случайной величины и её распределения вероятностей. Функция распределения и её свойства. Классификация случайных величин. Интеграл Лебега по вероятностной мере. Математическое ожидание, дисперсия, ковариация, энтропия, количество информации.

11. Законы больших чисел, центральная предельная теорема.

Понятие о случайной последовательности и видах её сходимости; соотношения между видами сходимости. Закон больших чисел: критерий, теоремы Маркова, Чебышева. Усиленный закон больших чисел: теорема Линдеберга-Феллера и её следствия.

12. Стационарные и марковские случайные процессы, их свойства и применения.

Стационарные случайные процессы. Ковариационная функция, спектральная плотность и их свойства. Условия непрерывности и дифференцируемости в среднеквадратическом. Определение, классификация и свойства марковских

случайных процессов. Цепь Маркова с дискретным временем: вероятности p -шаговых переходов, эргодическая теорема.

13. Статистические оценки параметров, их свойства и методы построения.

Понятие точечной оценки; состоятельность, несмещенность, вариация оценки. Методы построения точечных оценок и их свойства: метод моментов, метод максимального правдоподобия, метод наименьших квадратов, байесовский метод. Понятие интервальной оценки; методы построения: метод обратной функции, метод “ t -студентизации”, асимптотически наикратчайшие интервалы.

14. Методы статистической проверки гипотез.

Постановка задачи статистической проверки гипотез. Фундаментальная лемма Неймана-Пирсона. Риск принятия решений. Байесовское решающее правило.

15. Постановка основных краевых задач для уравнений в частных производных и методы их решения

Задача Коши для уравнения гиперболического типа, метод характеристик, формула Даламбера. Задача Коши для уравнения параболического типа, метод интегральных преобразований. Смешанные задачи для уравнений гиперболического, параболического типа, метод разделения переменных. Простейшие сеточные методы.

16. Матричные игры и методы их решения. Игры с природой.

Понятие конфликтной ситуации. Определение матричной игры. Принцип НЭША. Решение матричных игр в чистых стратегиях. Решение матричных игр в смешанных стратегиях. Геометрические методы решения матричных игр.

17. Сетевые графики и их анализ.

Параметры сетевых графиков. Алгоритмы нахождения минимального и максимального времени наступления событий. Алгоритм нахождения критического пути.

18. Симплекс-метод как основной метод решения задач линейного программирования.

Постановка задачи Геометрическая интерпретация решения. Базисный план. Потенциалы, оценки. Критерий оптимальности. Двойственная задача к канонической и нормальной формам. Физический смысл двойственных переменных.

19. Метод множителей Лагранжа в нелинейном и выпуклом программировании. Теорема Куна-Таккера.

Постановка задачи нелинейного программирования со смешанными ограничениями. Понятие регулярного (нормального) 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.

20. 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). Другие примеры применения метода динамического программирования.

21. Приближение функций.

Наилучшее среднеквадратичное приближение. Метод наименьших квадратов. Интерполирование. Основные представления интерполяционного многочлена и остатка интерполирования. Сплайн-интерполирование.

22. Графы. Основные классы графов. Базовые алгоритмы поиска на графах и их трудоемкость.

Определение графа. Способы задания графов. Изоморфизм графов. Деревья и их свойства. Двудольные графы и критерий двудольности. Плоские и планарные графы. Формула Эйлера. Гомеоморфные графы. Критерий планарности Понтрягина – Куратовского. Эйлеровы графы и критерий эйлеровости. Гамильтоновы циклы и цепи. Достаточные условия гамильтоновости графов. Базовые алгоритмы поиска на графах и их трудоемкость (поиск в глубину и ширину, алгоритмы построения минимального остовного дерева и кратчайших маршрутов).

II. КОМПЬЮТЕРНЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

23. Основные типы данных в языках программирования и операции над ними.

Стандартные типы данных и их характеристики. Простые и структурированные типы. Порядковые, перечислимые, множественные типы. Массивы. Записи. Строковые типы. Классы и объекты. Пользовательские типы данных. Совместимость типов. Приведение типов. Ввод-вывод данных. Операции над данными.

24. Основные понятия объектно-ориентированного программирования. Реализация концепций ООП в различных языках программирования. Библиотеки классов.

Классы и объекты. Инкапсуляция, наследование, полиморфизм. Виртуальные методы и абстрактные классы. Раннее и позднее связывание. Организация доступа к элементам класса. Конструкторы, деструкторы. Библиотеки классов.

25. Процессы и ресурсы. Взаимодействие и синхронизация вычислительных процессов.

Понятие процесса и ресурса. Алгоритмы планирования процессов. Реализация механизмов взаимодействия процессов (критические секции, семафоры, мьютексы). Обработка тупиковых ситуаций: распознавание, обход и предотвращение тупиков.

26. Проектирование БД. Структура и основные функции СУБД.

Модели данных. Этапы проектирования БД. Нормализация отношений. Первая, вторая, третья и усиленная третья нормальные формы. Основные компоненты СУБД. Поддержка языков баз данных. Управление транзакциями. Журнализация и восстановление БД. Локальные и распределенные БД.

27. Модели, протоколы, технические средства построения компьютерных сетей.

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

28. 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.

III. СПЕЦИАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

29. 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 энтропии на классе вероятностных распределений. Количество информации по Шеннону и его свойства.

30. Теоретическая и практическая стойкость шифров по Шеннону.

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

31. 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.

32. 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.

33. 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.

34. 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: p -метод, метод $p - 1$, квадратичное решето.

35. Электронная цифровая подпись.

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

36. Программно-аппаратные средства защиты информации.

Требования к средствам криптографической защиты информации (FIPS 140–2). Методы и средства хранения ключевой информации. Защита от изменения и контроль целостности. Программно-аппаратные средства защиты ПЭВМ.

37. Теоретические основы информационной безопасности.

Модели и политики безопасности. Угрозы и уязвимости информационных систем. Оценка защищенности средств вычислительной техники и автоматизированных информационных систем. Особенности применения криптографических методов. Менеджмент информационной безопасности.

38. Правовые основы информационной безопасности, стандартизация, лицензирование, сертификация.

Принципы и методы правового регулирования отношений в области информационной безопасности. Законодательство в области обеспечения информационной безопасности. Правовая защита информации, информационных ресурсов и информационных систем. Преступления против информационной безопасности. Стандарты информационной безопасности.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Подготовка к государственному экзамену по специальности предполагает обзор и приведение в систему сведений и знаний, полученных студентами за время учебы в университете. Каждый экзаменационный вопрос затрагивает большой раздел или несколько разделов ранее изученных дисциплин. Отвечая на вопросы государственного экзамена, студент должен продемонстрировать грамотное изложение соответствующего материала и свое видение того, какое место и значение занимает этот материал во всем комплексе полученных знаний.

Студентам создаются необходимые условия для подготовки к государственному экзамену. При подготовке к государственному экзамену следует пользоваться литературой, рекомендованной в учебных программах соответствующих учебных дисциплин, методическими материалами кафедр, размещенными в открытом доступе на сайте факультета (учебные пособия, курсы лекций, мультимедийные презентации, методические указания, задания в тестовой форме для самоконтроля и др.).

Представленная Программа подготовки к государственному экзамену по специальности помимо экзаменационных вопросов содержит пояснения, которые носят рекомендательный характер. Студент вправе изложить свое понимание экзаменационного вопроса и свой личный взгляд на структуру и содержание ответа на данный вопрос. Экзаменационные билеты будут содержать только вопросы.

ЛИТЕРАТУРА

1. *Ахо, А. В.* Структуры данных и алгоритмы / А. В. Ахо, Д. Э. Хопкрофт, Д. Д. Ульман. : Учеб. пособие/ пер. с англ. М. : Вильямс, 2000. – 384 с.
2. *Богданов Ю.С.* Лекции по математическому анализу. – Мн.: изд-во БГУ, 1974, 1978. – Ч.1-2.
3. *Богданов, Ю.С.* Математический анализ / Ю.С. Богданов, О. А. Кастрица, Ю. Б. Сыроид – М.: ЮНИТИ-ДАНА, 2003. – 351 с.
4. *Богданов, Ю.С.* Дифференциальные уравнения / Ю. С. Богданов, Ю. Б. Сыроид – Мн.: Выш. школа, 1983. – 239 с.
5. *Богданов, Ю.С.* Курс дифференциальных уравнений / Ю. С. Богданов, С. А. Мазаник, Ю. Б. Сыроид – Мн.: Университетское, 1996. – 287 с.
6. *Вагнер Г.* Основы исследования операций: в 3-х томах. М.: Мин, 1972-73.– 335 с., – 487 с., – 501 с.
7. *Вентцель Е. С.* Исследование операций. М.: Сов. Наука, 1972. – 550 с.
8. *Воеводин, В.В.* Параллельные вычисления / В. В. Воеводин, Вл. В. Воеводин. СПб. : БХВ-Петербург, 2002. – 608 с.
9. *Воробьев Н.Н.* Теория игр. Ленинград: ЛГУ, 1975. – 324.
10. *Габасов, Р.* Методы оптимизации: Учебное пособие / Р. Габасов, Ф. М. Кириллова – Мн.: Изд-во БГУ, 1981. – 350 с.
11. *Гамма, Э.* Приемы объектно-ориентированного проектирования. Паттерны проектирования / Гамма Э., Хелм Р., Джонсон Р., Влиссидс Дж. — СПб.: Питер, 2007. — 366 с. — (Серия "Библиотека программиста").
12. *Дегтярев Ю.И.* Исследование операций. М.: Высшая школа, 1986. – 319с.
13. *Дейт К. Дж.* Введение в системы баз данных — 8-е изд. — М.: Вильямс, 2006. — 1328 с.
14. *Демидович Б.П.* Сборник задач и упражнений по математическому анализу. – М.: Наука, 1998. – 624с.
15. *Емеличев, В. А.* Лекции по теории графов/ В. А. Емеличев, О. И. Мельников, В. И. Сарванов, Р. И. Тышкевич. – М.: Наука, 1990. – 383 с.
16. *Зорич В. А.* Математический анализ.– М.: Наука, 1997, 1998. – Ч.1-2
17. *Игошин В. И.* Теория алгоритмов: учеб. пособие для студ. высш. учеб. заведений / В. И. Игошин. ИНФРА-М, 2012. – 318 с.
18. *Ильин, В.А.* Математический анализ / В.А. Ильин, В.А. Садовничий, Бл. Х. Сендов. – М.: изд-во Моск. ун-та, 1985, 1987. – Ч.1–2.
19. *Иржавский, П. А.* Теория алгоритмов: учеб. пособие / П. А. Иржавский, В.М. Котов, А.Ю. Лобанов, Ю.Л. Орлович, Е.П. Соболевская – Минск : БГУ, 2013. – 159 с.
20. *Кормен, Т.* Алгоритмы : построение и анализ/ Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн. М. : Вильямс, 2005. 1296 с.

21. *Котов, В. М.* Алгоритмы и структуры данных: учеб. пособие / В.М. Котов, Е.П. Соболевская, А.А. Толстиков – Минск : БГУ, 2011. – 267 с. – (Классическое университетское издание).
22. *Краснов, М. Л.* Функции комплексного переменного. Операционное исчисление. Теория устойчивости. / М.Л. Краснов, А.И. Киселёв, Г.И. Макаренко – М.: Наука, 1981. – 303с.
23. *Крылов, В.И.* Вычислительные методы высшей математики / В. И. Крылов, В. В. Бобков, П. И. Монастырный – Мн.: Выш. школа, 1972.– 594 с.
24. *Крылов, В.И.* Вычислительные методы / В. И. Крылов, В. В. Бобков, П. И. Монастырный – Том 1, М.: Наука, 1972.– 594 с.
25. *Кудрявцев Л.Д.* Курс математического анализа.– М.: Высш. шк.: 1988, 1988, 1989.– Т.1-3.
26. *Липский В.* Комбинаторика для программистов. – М.: Мир, 1988. – 214с.
27. *Лиходед Н. А.* Методы распараллеливания гнезд циклов: курс лекций. - Минск : БГУ, 2008. – 100 с.
28. *Олифер, В.* Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер — 4-е изд. — СПб.: Питер, 2014. — 944 с. — (Серия «Классика computer science»).
29. *Пападдимитриу, Х.* Комбинаторная оптимизация: Алгоритмы и сложность/ Х. Пападдимитриу, К. Стайглиц. – М.: Мир, 1971. – 512 с.
30. *Размыслович, Г. П.* Геометрия и алгебра / Г. П. Размыслович, М. М. Феденя, В. М. Ширяев – Мн.: Университетское, 1987.– 350 с.
31. *Размыслович, Г. П.* Сборник задач по геометрии и алгебре / Г. П. Размыслович, М. М. Феденя, В. М. Ширяев – Мн.: Университетское, 1999.– 384 с.
32. *Рейнгольд, Э.* Комбинаторные алгоритмы теория и практика/ Э. Рейнгольд, Ю. Нивергельт, Н. Део. – М.: Мир, 1980. – 476 с.
33. *Сидоров, Ю.В.* Лекции по теории функций комплексного переменного / Ю.В. Сидоров, М.В. Федорюк, М.И. Шабунин. – М.: Наука, 1989. – 408с.
34. *Стенли Р.* Перечислительная комбинаторика. М.: Мир, 1990. – 440 с.
35. *Танаев, В.С.* Введение в теорию расписаний / В. С. Танаев, В. В. Шкурба – М.: Наука, 1975.– 256 с.
36. *Таненбаум Э.* Современные операционные системы — 3-е изд. — СПб.: Питер, 2010. — 1120 с. — (Серия «Классика computer science»).
37. *Таненбаум, Э.* Компьютерные сети / Таненбаум Э., Уэзеролл Д. — 5-е изд. — СПб.: Питер, 2014. — 960 с. — (Серия "Классика computer science").
38. *Таха Х. А.* Введение в исследование операций. М., С.–Петербург, Киев: Изд. Дом Вильямс, 2001. – 911 с.
39. *Тер-Криков, А. М.* Курс математического анализа / А. М. Тер-Криков, М. И. Шабунин – М.: Наука, 1997. – 720с.
40. *Тышкевич, Р.И.* Линейная алгебра и аналитическая геометрия / Р. И. Тышкевич, А. С. Феденко – Мн.: Выш. школа, 1976. – 544 с.
41. *Форд, Л.* Потоки в сетях / Форд Л., Фалкерсон Д. – Мир, 1966.– 276 с.

42. Харин, Ю. С. Математическая и прикладная статистика / Ю. С. Харин, Е. Е. Жук – Мн.: БГУ, 2005. – 279 с.
43. Харин, Ю. С. Теория вероятностей / Ю. С. Харин, Н. М. Зуев – Мн.: БГУ, 2004. – 199 с.
44. Ширяев А. Н. Вероятность. В 2-х кн. – Москва: МЦНМО, 2004. – 928 с.
45. Яблонский С.В. Введение в дискретную математику. – М.: Наука, 1979. – 272 с.