УТВЕРЖДЕНО
Решением Ученого совета факультета
математики, информационных и авиационных технологий
от «21» 06 2019 г., протокол № 5/13
Председатель Веселов М.И.
«21» 06 2019 г.

РАБОЧАЯ ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Аттестация	Государственная итоговая аттестация
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	6

Специальность: 10.05.01 «Компьютерная безопасность»
код направления (специальности), полное наименование

Специализация: «Математические методы защиты информации»
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «01» 09 2019 г.

Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Рацеев Сергей Михайлович	ИБиТУ	профессор, д.ф-м.н, доцент

СОГЛАСОВАНО
Заведующий выпускающей кафедрой
_____ / А.С. Андреев / (Подпись) (Ф.И.О.) «13» 06 2019 г.

1. ЦЕЛИ И ЗАДАЧИ ГИА

Государственная итоговая аттестация (ГИА) по специальности «Компьютерная безопасность» позволяет выявить и оценить теоретическую и практическую подготовку выпускника к решению профессиональных задач, готовность к основным видам профессиональной деятельности.

Цель проведения ГИА состоит в проверке знаний и навыков студента, полученных им в процессе обучения, и оценке его профессионального уровня по специальности «Компьютерная безопасность».

Задачи ГИА:

– проверка знания студентом основных теоретико-методологических подходов и уровня освоения базовых предметов специальности, определяющих профессиональные способности выпускника;

– оценка умения студента ориентироваться в текущей ситуации в области информационной безопасности;

– оценка уровня обоснования студентом собственных выводов, грамотности их изложения;

– определение соответствия подготовки выпускников квалификационным требованиям федерального государственного образовательного стандарта высшего образования (далее по тексту ФГОС ВО).

2. МЕСТО ГИА В СТРУКТУРЕ ОПОП ВО

Данный модуль входит в блок «Государственная итоговая аттестация» Основной Профессиональной Образовательной Программы по специальности «Компьютерная безопасность» и включает в себя государственный экзамен и защиту выпускной квалификационной работы (ВКР). Для успешного освоения ГИА используются знания, умения, навыки и компетенции, сформированные в процессе обучения по базовым дисциплинам указанной специальности.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО МОДУЛЮ, СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Программа ГИА направлена на определение сформированности у выпускников следующих компетенций:

общекультурными компетенциями:

– способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

– способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

– способностью анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

– способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

– 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 (ОК-5);

– способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

– способностью к 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 (ОК-7);

– способностью к самоорганизации и самообразованию (ОК-8);

– способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

общепрофессиональными компетенциями:

– способностью анализировать физические явления и процессы при решении профессиональных задач (ОПК-1);

– способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

– способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

– способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);

– способностью использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);

– способностью применять приемы первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-6);

– способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7);

– способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8);

– способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);

– способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).

профессиональными компетенциями:

– способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов**,** отечественного и зарубежного опыта по проблемам компьютерной безопасности (ПК-1);

– способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований (ПК-2);

– способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности (ПК-3);

– способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПК-4);

– способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управ-

ления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);

– способностью участвовать в разработке проектной и технической документации (ПК-6);

– способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-7);

– способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы (ПК-8);

– способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы (ПК-9);

– способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-10);

– способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации (ПК-11);

– способностью проводить инструментальный мониторинг защищенности компьютерных систем (ПК-12);

– способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-13);

– способностью организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа (ПК-14);

– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-15);

– разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем (ПК-16);

– способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение (ПК-17);

– способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18);

– способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации (ПК-19);

– способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций (ПК-20);

профессионально-специализированными компетенциями:

– способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации (ПСК-2.1);

– способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах (ПСК-2.2);

– способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов (ПСК-2.3);

– способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты

информации (ПСК-2.4);

– способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации (ПСК-2.5).

При сдаче государственного экзамена студент должен:

Знать:

– основные понятия и методы математического анализа, геометрии, алгебры, теории функций комплексного переменного, теории вероятностей и математической статистики;

– принципы организации информационных систем в соответствии с требованиями информационной защищенности, в том числе в соответствии с требованиями по защите государственной тайны;

– базовый понятийный аппарат в области информационной безопасности и защиты информации;

– виды и состав угроз информационной безопасности;

– конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, потенциальные каналы утечки информации, характерные для этих устройств, способы их выявления и методы оценки опасности, основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;

– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

– принципы построения современных криптографических систем, стандарты в области криптографической защиты информации;

– основные правовые положения в области информационной безопасности и защиты информации;

– виды уязвимости защищаемой информации и формы ее проявления;

– каналы и методы несанкционированного доступа к конфиденциальной информации;

– наиболее уязвимые для атак противника элементы компьютерных систем;

Владеть:

– методами организации и управления деятельностью служб защиты информации на предприятии;

– технологией проектирования, построения и эксплуатации комплексных систем защиты информации;

– методами научного исследования уязвимости и защищенности информационных процессов;

– методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;

– навыками использования типовых криптографических алгоритмов;

– навыками математического моделирования в криптографии;

– навыками самостоятельной работы с современными международными стандартами криптографических протоколов;

Применять и осуществлять на практике:

– основные методы математического, комплексного анализа, алгебры и геометрии;

– комплекс мер по информационной безопасности с учетом его правовой обоснованности;

– разработку математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов;

– проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средствах защиты информации;

– применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;

– проведение инструментального мониторинга защищенности компьютерных систем;

– организацию работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих государственную тайну и конфиденциальной информации).

4. ОБЩАЯ ТРУДОЕМКОСТЬ ГИА

Общая трудоемкость ГИА составляет 324 часа (9 зачетных единиц). Из них:

- 108 часов (3 ЗЕ) отводится на подготовку и сдачу государственного экзамена,
- 216 часов (6 ЗЕ) отводится на подготовку и защиту ВКР.

5. ПРОГРАММА ГИА

В блок "Государственная итоговая аттестация" входит

- подготовка к сдаче и сдача государственного экзамена,
- защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

В программу государственного экзамена включены темы и вопросы по дисциплинам учебного плана по специальности «Компьютерная безопасность», определяющие базис формирования профессиональных компетенций выпускника.

Государственный экзамен проводится по билетам в устной форме. Каждый билет состоит из пяти заданий: три теоретических и два практических. Вопросы носят теоретический (проверяют уровень подготовки по основным профессиональным дисциплинам) и практический (обеспечивают проверку уровня профессиональных знаний и умение решать практические задачи, типичные для области профессиональной деятельности) характер.

6. ПЕРЕЧЕНЬ ВОПРОСОВ К ГОСУДАРСТВЕННОМУ ЭКЗАМЕНУ

ЧАСТЬ 1. МАТЕМАТИКА

Раздел 1. Математический анализ

1. Предел и непрерывность функций одной и нескольких переменных. Свойства функций, непрерывных на отрезке.

2. Производная и дифференциал функций одной и нескольких переменных. Достаточные условия дифференцируемости. Теорема Ферма. Теоремы Ролля, Лагранжа и Коши.

3. Формула Тейлора с остаточным членом в форме Лагранжа и Коши. Формулы Тейлора основных элементарных функций. Экстремумы функций одной переменной. Достаточные условия экстремума.

4. Первообразная и неопределенный интеграл. Определенный интеграл, его свойства. Необходимые и достаточные условия интегрируемости. Основная формула интегрального исчисления.

5. Числовые ряды. Абсолютная и условная сходимость числового ряда. Признаки сходимости числового ряда: признак Даламбера, интегральный признак Коши-Маклорена, теорема Лейбница для знакочередующихся рядов.

6. Степенные ряды. Теорема Абеля. Радиус сходимости, интервал сходимости степенного ряда. Теорема Коши-Адамара. Разложение элементарных функций в ряд Тейлора.

Раздел 2. Алгебра и геометрия

7. Матрицы и операции над ними. Определители матриц и их свойства. Определитель Вандермонда. Ранг матрицы. Критерий обратимости матриц. Способы вычисления обратной матрицы.

8. Векторные пространства, их базисы и размерность. Критерий подпространства. Координаты векторов в базисе и их изменение при переходе к другому базису.

9. Системы линейных алгебраических уравнений. Теорема Кронекера-Капелли. Общее решение системы линейных алгебраических уравнений.

10. Линейные преобразования векторного пространства и их матрицы. Характеристический многочлен линейного преобразования. Собственные значения и собственные векторы.

11. Евклидовы пространства. Процесс ортогонализации. Ортогональные преобразования евклидова пространства. Ортогональные матрицы и их свойства.

12. Группы и их основные свойства. Циклические группы. Смежные классы по подгруппе. Теорема Лагранжа. Морфизмы групп.

13. Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца. Идеал кольца. Фактор-кольцо. Кольца вычетов.

14. Кольцо многочленов. Наибольший общий делитель и наименьшее общее кратное. Свойства наибольшего общего делителя двух многочленов. Алгоритм Евклида.

15. Конечные поля. Характеристика поля. Построение конечного поля с заданным числом элементов.

16. Прямая и плоскость, их уравнения. Взаимное расположение прямой и плоскости. Основные задачи на прямую и плоскость.

Раздел 3. Дискретная математика

17. Основные комбинаторные величины. Булеан. Размещения и сочетания (с повторением и без повторения). Числа Стирлинга первого и второго рода.

18. Булева алгебра. Понятие булевой функции. Представление булевой функции в виде СДНФ, СКНФ, полиномов Жегалкина. Теорема Поста о полноте системы булевых функций.

19. Понятие графа и связанные с ним определения. Виды представления графа. Полные и двудольные графы. Критерий двудольности графов. Эйлеровы и гамильтоновы графы.

Раздел 4. Теория вероятностей и математическая статистика

20. Вероятностное пространство. Свойства вероятностной меры. Классическое определение вероятности. Условные вероятности. Независимость событий. Формула полной вероятности. Формула Байеса.

21. Случайные величины. Функции распределения случайных величин и их свойства. Плотности распределения. Типовые распределения случайных величин: биномиальное, геометрическое, пуассоновское, равномерное, нормальное.

22. Математическое ожидание и дисперсия случайных величин: определения и основные свойства. Математическое ожидание и дисперсия типовых распределений случайных величин.

23. Статистики, статистические оценки и их свойства. Методы статистического оценивания неизвестных параметров: метод максимального правдоподобия, метод моментов. Основные типы статистических гипотез. Общая логическая схема статистического критерия.

Раздел 5. Теория функций комплексного переменного

24. Комплексные числа. Тригонометрическая форма комплексных чисел. Формула Муавра. Извлечение корней. Производная функции комплексного переменного. Условия Коши-Римана. Аналитическая функция. Формула Эйлера.

Раздел 6. Теоретико-числовые методы в криптографии

25. Отношение делимости в кольце целых чисел и его свойства. Наибольший общий делитель и его свойства.

26. Алгоритм Евклида. Обобщенный алгоритм Евклида. Линейные диофантовы уравнения первой степени.

27. Простые числа и их свойства. Решето Эратосфена. Основная теорема арифметики.

28. Мультипликативные функции и их свойства. Функция Эйлера и ее свойства.

29. Отношение сравнимости в кольце целых чисел и его свойства. Полная и приведенная системы вычетов. Теорема Эйлера. Малая теорема Ферма.

30. Сравнения первой степени, методы их решений. Системы сравнений первой степени. Китайская теорема об остатках.

31. Сравнения второй степени. Квадратичные вычеты и невычеты. Символ Лежандра. Символ Якоби.

32. Степенные вычеты. Показатель числа. Первообразные корни по простому модулю.

33. Вероятностные методы проверки простоты натурального числа. Тест Соловея-Штрассена. Тест Миллера-Рабина.

34. Методы дискретного логарифмирования в конечном поле.

35. Эллиптические кривые. Сложение точек эллиптической кривой над полем. Аддитивная группа точек эллиптической кривой. Порядок точки.

ЧАСТЬ 2. ЗАЩИТА ИНФОРМАЦИИ

Раздел 7. Основы информационной безопасности

36. Классификация угроз информации. Источники угроз информационной безопасности РФ. Модель действий нарушителя.

37. Понятие информационной войны. Составные части и методы информационного противоборства. Информационное оружие.

38. Концепция защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности.

39. Направления защиты от несанкционированного доступа (НСД). Основные способы НСД. Структура системы защиты информации от НСД, назначение и функции элементов.

40. Правила разграничения доступа к информации. Мандатная и дискреционная модели управления доступом.

41. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Основные методы аутентификации.

42. Технология межсетевых экранов (МЭ). Виды МЭ.

43. Основные понятия и функции виртуальных частных сетей (VPN).

Раздел 8. Криптографические методы защиты информации

44. Совершенные по Шеннону шифры. Необходимые и достаточные условия совершенных шифров. Теорема К.Шеннона. Табличное и модульное гаммирование.

45. Имитация и подмена шифрованных сообщений. Оценки для вероятностей имитации и подмены сообщений. Критерии достижимости нижних оценок.

46. Симметричные блочные шифры. Шифры Фейстеля и их обратимость. Шифр “Магма” из ГОСТ Р 34.12-2015.

47. Шифр “Кузнечик” из ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров.

48. Асимметричные шифры. Схема Диффи-Хеллмана. Шифр RSA. Шифр Эль-Гамаля. Шифр Месси-Омуры.

49. Модификация асимметричных шифров на эллиптических кривых. Модификация схемы Диффи-Хеллмана. Модификация шифра Эль-Гамаля. Модификация шифра Месси-Омуры.

50. Хеш-функции. Требования, предъявляемые к хеш-функциям. Криптографические хеш-функции. Способы построения криптографических хеш-функций.

51. Коды аутентификации. Понятие имитации и подмены сообщения. Нижние оценки для вероятностей успеха имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации.

52. Электронная подпись. Электронная подпись на основе асимметричных систем шифрования: электронная подпись RSA, электронная подпись Фиата-Шамира, электронная подпись Эль-Гамаля, электронная подпись Шнорра.

Раздел 9. Криптографические протоколы

53. Протоколы аутентификации, использующие пароли. Протоколы аутентификации, использующие технику “запрос-ответ”.

54. Протоколы аутентификации, использующие технику доказательства знания с нулевым разглашением: общие положения. Протокол Шнорра. Протокол Фиата-Шамира.

55. Модификация протоколов аутентификации на эллиптических кривых: модификация протокола Шнорра, модификация протокола Окамото.

56. Протоколы передачи ключей. Передача ключей с использованием симметричного шифрования. Протокол Kerberos. Передача ключей с использованием асимметричного шифрования. Сертификаты открытых ключей.

57. Протоколы передачи ключей. Открытое распределение ключей. Протокол Диффи-Хеллмана и его усиления. Предварительное распределение ключей.

58. Схемы разделения секрета. Схема Шамира. Схема Ито-Саито-Нишизеки.

Раздел 10. Теория кодирования, сжатия и восстановления информации

59. Линейные коды: основные понятия. Критерии обнаружения и исправления ошибок. Код Хемминга.

60. Декодирование линейного кода. Синдромы, свойства синдромов, синдромное декодирование. Стандартное расположение для кода.

61. Коды Боуза-Чоудхури-Хоквингема. Кодирование и декодирование кодов БЧХ.

62. МДР коды. Коды Рида-Соломона. Кодирование и декодирование кодов РС.

Раздел 11. Теория псевдослучайных генераторов

63. Линейные конгруэнтные генераторы псевдослучайных последовательностей. Теорема о максимальной длине периода линейной конгруэнтной последовательности. Потенциал линейной конгруэнтной последовательности.

64. Генераторы на регистрах сдвига с линейными обратными связями. Принцип работы. Конфигурации Фибоначчи и Галуа. Теорема о максимальном периоде для генератора на регистрах сдвига с линейными обратными связями в данных конфигурациях.

Раздел 12. Защита программ и данных

65. Методы защиты программных реализаций от изучения.

66. Программные закладки. Пути внедрения программных закладок.

Раздел 13. Модели безопасности компьютерных систем

67. Модель Харрисона-Руззо-Ульмана. Основные понятия, свойства и анализ безопасности для данной модели.

68. Классическая модель Take-Grant. Основные понятия, свойства и анализ безопасности для данной модели.

69. Модель Белла-ЛаПадула. Основные понятия, свойства и анализ безопасности для данной модели.

Раздел 14. Техническая защита информации

70. Типовая структура и виды технических каналов утечки информации. Классификация технических каналов утечки информации.

71. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале.

72. Методы пассивной и активной защиты утечки информации по акустическому (виброакустическому) каналу.

Раздел 15. Организационное и правовое обеспечение информационной безопасности

73. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности.

74. Виды и содержание тайн. Законодательная база охраны государственной, коммерческой и служебной тайн.

75. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных и первоочередные мероприятия по созданию системы защиты персональных данных на предприятии.

76. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации.

77. Методы и средства инженерной защиты объектов информатизации.

78. Программные и аппаратные средства защиты информации от несанкционированного доступа.

Методические указания при подготовке к государственному экзамену приводятся в:

Рацеев С. М. Методические указания для самостоятельной работы студентов при подготовке к государственной итоговой аттестации для студентов специальности 10.05.01 «Компьютерная безопасность» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 298 КБ). - Текст : электронный. Режим доступа: http://lib.ulsu.ru/MegaPro/Download/MObject/4683

7. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАДАНИЙ К ГОСУДАРСТВЕННОМУ ЭКЗАМЕНУ

Примерные варианты практических заданий по математическому анализу

1. Найти предел $\lim\limits_{x\to\infty}\dfrac{2+x-4x^3}{5+x^2+3x^3}$.
2. Найти предел $\lim\limits_{x\to\infty}\left(\dfrac{x^3}{2x^2-1}-\dfrac{x^2}{2x+1}\right)$.
3. Найти предел $\lim\limits_{x\to 0}\dfrac{\sin^2 5x}{4x^2}$.
4. Найти предел $\lim\limits_{n\to\infty}\left(1-\dfrac{8n}{n^2+1}\right)^{3n}$.
5. Пусть $f(x)=\ln\sqrt{\dfrac{1-x}{1+x}}$. Найти $f'(x)$.
6. Найти интеграл $\int\dfrac{dx}{\sqrt{1-2x}}$.
7. Найти интеграл $\int\sqrt[4]{(7x+5)^3}\,dx$.
8. Найти интеграл $\int x\ln x\,dx$.
9. Найти интеграл $\int xe^{-x}dx$.

10. Найти интеграл $\int \frac{x-3}{x^2-16}dx$.
11. Найти интеграл $\int\limits_{-1}^{1} \frac{xdx}{\sqrt{5-4x}}$.
12. Вычислить объем тела, образованного вращением фигуры, ограниченной линиями:
13. $y=-x^2+4, \quad y=0, \quad y=3$ вокруг оси Оу.
14. Исследовать числовой ряд $\sum\limits_{n=1}^{\infty}\frac{1}{\sqrt{n}}$ на сходимость.
15. Исследовать числовой ряд $\sum\limits_{n=1}^{\infty}\frac{9^{n-1}}{n!}$ на сходимость.
16. Исследовать числовой ряд $\sum\limits_{n=1}^{\infty}\frac{n\cdot 3^{n+1}}{n^2+2}$ на сходимость.
17. Исследовать числовой ряд $\sum\limits_{n=1}^{\infty}\frac{(-1)^n n}{n^2+7}$ на сходимость.
18. Вычислить интеграл или определить его расходимость $\int\limits_{1}^{+\infty}\frac{dx}{\sqrt[3]{x}}$.
19. Вычислить интеграл или определить его расходимость $\int\limits_{e}^{+\infty}\frac{dx}{x\ln^2 x}$.
20. Вычислить интеграл или определить его расходимость $\int\limits_{0}^{+\infty}(3x+2)^6 dx$.

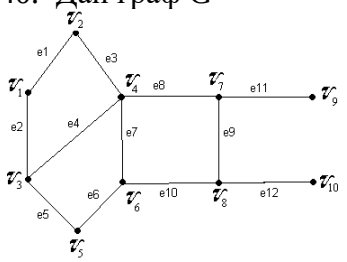
Примерные варианты практических заданий по алгебре и геометрии

21. На множестве $\mathbb{Z}$ определено бинарное отношение $\sim$ следующим образом: $a\sim b \Leftrightarrow 6|(a-b)$. Доказать, что $\sim$ является отношением эквивалентности. Найти разбиение множества $\mathbb{Z}$, которое индуцирует отношение $\sim$. Какому классу эквивалентности принадлежит элемент $a=-452$?
22. На множестве $M=\{4x|x\in\mathbb{N}\}$ определено бинарное отношение $\le$ следующим образом: $a\le b \Leftrightarrow a|b$. Проверить, является ли $\le$ отношением линейного порядка на M.
23. Проверить, является ли множество $\left\{\begin{pmatrix}8x & 0\\ 0 & 12y\end{pmatrix}|\, x,y\in\mathbb{Z}\right\}$ относительно операции сложения аддитивной абелевой группой.
24. Доказать, что множество $R=\{a+b\sqrt{3}\,|\,a,b\in\mathbb{Z}\}$ относительно операций сложения и умножения является коммутативным кольцом с единицей.
25. В мультипликативной группе кольца вычетов $\mathbb{Z}_{40}^{*}$ найти 29^{-1}.
26. Найти решения системы линейных алгебраических уравнений над полем $\mathbb{R}$:
$$\begin{cases} 2x_1 - x_2 + x_3 = -7,\\ -3x_1 - x_2 - 3x_3 = 7,\\ -2x_1 + x_2 - 2x_3 = 8. \end{cases}$$

27. Найти решения системы линейных алгебраических уравнений над кольцом вычетов по модулю 7: $\begin{cases} 3x_1 + 3x_2 + 6x_3 = 5, \\ 5x_1 + 3x_2 + 4x_3 = 2, \\ 6x_1 + x_2 + x_3 = 3. \end{cases}$
28. Доказать, что векторы $\bar{\mathbf{p}} = (0,1,2)$, $\bar{\mathbf{q}} = (1,0,1)$, $\bar{\mathbf{r}} = (-1,2,4)$ образуют базис арифметического пространства $\mathbb{R}^3$ и найти координаты вектора $\bar{\mathbf{a}} = (-2,4,7)$ в этом базисе.
29. Из векторов $\boldsymbol{a_1}$, $\boldsymbol{a_2}$, $\boldsymbol{a_3}$, $\boldsymbol{a_4}$ выбрать базу и разложить остальные по этой базе, где $\boldsymbol{a_1}$=(0,1, -3,4), $\boldsymbol{a_2}$ =(1, 0, -2,3), $\boldsymbol{a_3}$=(5, 2, -16, 23), $\boldsymbol{a_4}$=(1, -1,1, -1).
30. Над полем $\mathbb{R}$ найти многочлен Лагранжа $L(x)$, проходящий через точки $(-3,1)$, $(-1,5)$, $(3,-11)$. Вычислить $L(4)$ по схеме Горнера.
31. Пользуясь схемой Горнера, разложить многочлен $f(x)$ над полем $\mathbb{R}$ по степеням $x-c$, $f(x) = 4x^4 - 3x^3 - 2x^2 + 4x - 5$, $c = -2$.
32. Над кольцом вычетов по модулю 7 найти многочлен Лагранжа $L(x)$, проходящий через точки $(1,4)$, $(2,6)$, $(3,5)$.
33. Над полем $\mathbb{C}$ найти все корни многочлена $x^n - a$, где $n = 3$, $a = 2i$.
34. Найти координаты точек A и B, если известно, что точки $C(-15;12)$ и $D(-12;10)$ делят отрезок AB на три равные части.
35. Составить уравнение прямой, перпендикулярной $5x - 5y - 6 = 0$ и проходящей через точку пересечения прямых $2x - 5y - 7 = 0$ и $3x + 7y + 4 = 0$.
36. Найти точку пересечения прямой $\frac{x-2}{2} = \frac{y-1}{3} = \frac{z-3}{1}$ и плоскости $2x + 3y + z = 0$.
37. Записать уравнение плоскости, проходящей через точку $M_0(4;-1;1)$ перпендикулярно вектору $\overline{N} = \{-1;2;-2\}$. Найти острый угол, который эта плоскость образует с плоскостью $x + z - 6 = 0$.
38. Прямая проходит через точку $M_0(3,7,2)$ параллельно вектору $\overline{l} = (5;8;1)$. Записать уравнение прямой и указать, при каком значении C прямая будет параллельна плоскости $2x - y + Cz - 2 = 0$.
39. Записать уравнение прямой, проходящей через точки $M_1(-4;3;-3)$ и $M_2(2;-6;9)$. Доказать, что она пересекается с прямой $\frac{x-3}{3} = \frac{y-1}{4} = \frac{z-7}{2}$. Найти точку пересечения и угол между ними.

Примерные варианты практических заданий по дискретной математике

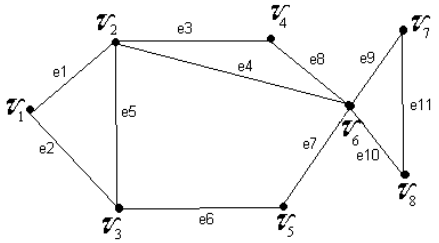
40. Дан граф G



1. Определить степени всех вершин графа.

2. Записать матрицу смежности вершин $A_1(G)$.
3. Записать матрицу инцидентности $A_2(G)$.
4. Определить цикломатическое число графа.
5. Построить каркас графа путем обхода «в ширину». Построить код.

41. Дан граф G



1. Определить степени всех вершин графа.
2. Записать матрицу смежности вершин $A_1(G)$.
3. Записать матрицу инцидентности $A_2(G)$.
4. Определить цикломатическое число графа.
5. Построить каркас графа путем обхода «в ширину». Построить код.

42. При помощи таблиц истинности найти СДНФ и СКНФ для $(x\,|(x \oplus y)) \downarrow \neg y$
43. При помощи таблиц истинности найти СДНФ и СКНФ для $x \vee ((x \downarrow y) \leftrightarrow (x \wedge y))$
44. При помощи таблиц истинности найти СДНФ и СКНФ для $((x \vee y) \leftrightarrow (\neg x \wedge z))|(y \oplus z)$

Примерные варианты практических заданий по теории вероятностей и математической статистике

45. В ящике лежат пять апельсинов и четыре яблока. Взяли три фрукта. С какой вероятностью все фрукты окажутся одного вида?
46. Первый стрелок попадает в цель с вероятностью 0.6, второй – с вероятностью 0.7. Первый стрелок делает 2 выстрела по мишени, а второй – 3 выстрела. С какой вероятностью не будет ни одного попадания в цель?
47. Завод имеет три источника поставки комплектующих – фирмы A, B, C. На долю фирмы A приходится 50% общего объема поставок, B – 30% и C – 20%. Среди поставляемых фирмой A деталей – 10% бракованных, фирмой B – 5% бракованных и фирмой C – 6%. С какой вероятностью взятая случайным образом деталь окажется пригодной?
48. Передается 4 сообщения по каналу связи. Каждое сообщение с вероятностью 0.1 искажается, независимо от других. Вычислить среднее число неискаженных сообщений. С какой вероятностью ровно три сообщения будут искажены?
49. В партии продукции, состоящей из 25 деталей, 5 бракованных. Определить вероятность того, что при случайном выборе четырех деталей: а) все они окажутся бракованными б) бракованных и не бракованных изделий будет поровну.
50. В автопробеге участвуют 3 автомобиля. Первый может сойти с маршрута с вероятностью 0,15; второй и третий автомобили не дойдут до финиша соответственно с вероятностью 0,05 и 0,1. Требуется определить вероятность того, что к финишу придут: а) только один автомобиль; б) два автомобиля; в) по крайней мере два автомобиля.
51. На сборку поступают детали с трех автоматов. Первый дает в среднем 98% годных деталей, второй – 99%, а третий – 97%. Найти вероятность попадания на сборку бракованной детали, если она выбрана случайным образом, а производительность автоматов одинакова.

Примерные варианты практических заданий по теории функций комплексного пере-

менного

52. Найти значение выражения $\frac{z_1 \cdot z_2 + z_3}{z_4}$, где $z_1 = 3+4i$, $z_2 = 5-4i$, $z_3 = -4-5i$, $z_4 = 4-2i$.
53. Вычислить значение выражения $\frac{z_1^m \cdot z_2^n}{z_3^k}$ и записать ответ в алгебраической форме, где $z_1 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, $z_2 = -\frac{\sqrt{3}}{2} - i\frac{1}{2}$, $z_3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, $m=7$, $n=13$, $k=8$.
54. Найти все корни $\sqrt[n]{z}$, $n=3$, $z=2i$.
55. Используя формулу Муавра, вычислить $\left(\frac{-1+i\sqrt{3}}{1-i}\right)^{10}$.
56. Найти корни уравнения и отметить их на комплексной плоскости $z^3 + i = 0$.
57. Найти корни уравнения и отметить их на комплексной плоскости $z^2 + 5 - 12i = 0$.

Примерные варианты практических заданий по теоретико-числовым методам в криптографии

58. Найти общее решение линейного диофантова уравнения $41x + 23y = 1$.
59. Найти общее решение линейного диофантова уравнения $43x+18y=3$.
60. Разложить рациональное число 129/53 в конечную цепную дробь.
61. Найти значение конечной цепной дроби [3;2,3,1,3].
62. Найти каноническое разложение числа 18! (факториал числа).
63. Найти число и сумму делителей, а также значение функции Эйлера числа 100.
64. Используя теорему Эйлера, найти остаток от деления числа 15^{175} на 11.
65. Используя теорему Эйлера, найти остаток от деления числа $3^{100} + 37^{100}$ на 16.
66. Вычислить обратный элемент, если он существует: $7^{-1} \bmod 41$.
67. Решить сравнение $7x \equiv 10 \pmod{19}$.
68. Решить сравнение $12x \equiv 4 \pmod{17}$.
69. Решить систему сравнений $\begin{cases} x \equiv 1 (\bmod 3), \\ x \equiv 2 (\bmod 5), \\ x \equiv 3 (\bmod 7). \end{cases}$
70. Вычислить, пользуясь свойствами символа Якоби $\left(\frac{82}{101}\right)$.
71. Решить квадратичное сравнение по простому модулю, если решение существует $x^2 \equiv 3 \pmod{11}$.
72. Найти все первообразные корни по модулю 11.

Примерные варианты практических заданий по дисциплине «Основы информационной безопасности»

73. Определить информационные активы выбранного предприятия, основные угрозы для них и способы (средства) их нейтрализации.
74. Разработать план занятия с пользователями ПЭВМ предприятия по обучению работе с электронным замком «СОБОЛЬ».
75. Разработать план занятия с пользователями ПЭВМ предприятия по обучению работе с комплексом средств защиты информации от несанкционированного доступа «АККОРД».
76. Разработать план занятия с пользователями ПЭВМ предприятия по обучению работе с персональными средствами аутентификации и защищенного хранения данных (USB-ключи и смарт-карты eToken).
77. Разработать план занятия с пользователями ПЭВМ предприятия по обучению работе с

системой защиты «Dallas Lock 8.0-K(C)».

Примерные варианты практических заданий по криптографическим методам защиты информации

78. Шифр Месси-Омуры. Пусть a_1, a_2 – пара секретных ключей абонента *A*, b_1, b_2 – пара секретных ключей абонента *B*, *p* – простое число, *m* – передаваемое сообщение от *A* к *B*. Известно, что $p=7$, $a_1=3$, $b_1=5$, $m=2$. Найти a_2, b_2, m_1, m_2, m_3.
79. Шифр Эль-Гамаля. Пусть *x*, *y* – соответственно секретный и открытый ключи абонента *A*, *p* – простое число, *g* – первообразный корень по модулю *p* (параметры шифрсистемы), *m* – передаваемое сообщение абоненту *A*, *k* – случайное число. Известно, что $p=7$, $g=3$, $x=5$, $k=4$, $m=2$. Найти *y* и шифрованное сообщение (c_1,c_2), передаваемое абоненту *A*.
80. Шифр RSA. Пусть *d*, *e* – соответственно секретный и открытый ключи абонента *A*, *p*, *q* – простые числа абонента *A*, *m* – передаваемое сообщение абоненту *A*. Известно, что $p=3$, $q=7$, $e=3$, $m=2$. Найти *d* и шифрованное сообщение *y*, передаваемое абоненту *A*.

Примерные варианты практических заданий по криптографическим протоколам

81. Восстановить значение секрета *s* в схеме Шамира с порогом 2 над кольцом вычетов по модулю 11, если доли двух участников, пытающихся восстановить секрет, равны: (3, 3), (7, 8)
82. Пусть $s=3$ – секрет. Какие доли данного секрета получит каждый участник (4,2)-пороговой схемы разделения секрета на основе равновесных двоичных кодов.
83. Схема Ито-Саито-Нишизеки. Пусть $P=\{1,2,3,4\}$ – участники разделения секрета *s*, (*R*,*Z*) – структура доступа на *P*, которая задается множеством минимальных правомочных коалиций $R_{\min} = \{\{1, 2, 3\}, \{2, 4\}, \{3, 4\}\}$. Найти множество максимальных непровомочных коалиций $Z_{\max}$ (выписать в лексикографическом порядке), кумулятивный массив *C*, а также разделить секрет $s=5$ (выписать доли секрета для каждого участника).
84. Протокол Фиата-Шамира. Пусть $n = p \cdot q$ – параметр протокола, x, y – соответственно секретный и открытый ключи доказывающего абонента A, k – случайный параметр из первого шага протокола, a – запрос из второго шага протокола. Найти y и привести все вычисления на четырех шагах протокола (найти r, s, проверить соответствующее сравнение) если известно, что p=3, q=7, a=1, x=2, k=10.
85. Протокол Шнорра. Пусть p – простое число, q – простой делитель числа $p-1$, g – элемент из кольца вычетов по модулю p (имеющий порядок q), x, y – соответственно секретный и открытый ключ абонента A, k – случайное число из первого шага протокола. Известно, что $p=7, q=3, g=2, a=1, x=2, k=2$. Найти y и привести все вычисления на четырех шагах протокола (найти r, s проверить соответствующее сравнение).

Примерные варианты практических заданий по теории кодирования, сжатию и восстановлению информации

86. Построить поле $GF(2^3)$ на основе примитивного многочлена x^3+x+1 с примитивным элементом α.
87. Проверочная матрица (7,4,3)-кода Хэмминга задается в лексикографическом порядке слева направо по возрастанию. На приемном конце получен вектор $v=\begin{pmatrix}1 & 1 & 0 & 0 & 0 & 1 & 0\end{pmatrix}$. Исправить ошибку и найти кодовый вектор u.
88. Порождающая матрица линейного (5,2,3)-кода с параметрами $n=5$, $k=2$ имеет вид $G=\begin{pmatrix}1 & 1 & 0 & 1 & 0\\ 0 & 1 & 1 & 1 & 1\end{pmatrix}$. Найти проверочную матрицу H, кодовое расстояние d. Составить таблицу стандартного расположения. С помощью данной таблицы декодировать вектор $v=\begin{pmatrix}0 & 0 & 1 & 0 & 1\end{pmatrix}$, т.е. найти информационный вектор i.

89. Поле $GF(2^4)$ строится с помощью примитивного многочлена x^4+x+1, α – примитивный элемент. Двоичный код БЧХ с параметрами $n=15$, $k=7$ порождается многочленом $g(x)=1+x^4+x^6+x^7+x^8$, $\alpha,\alpha^2,\alpha^3,\alpha^4$ – его подряд идущие корни. На приемном конце получен вектор $v=(1,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1,\ 0,\ 1)$, в котором не более двух ошибок. Найти соответствующий кодовый вектор u и информационный вектор i.
90. Поле $GF(3^2)$ строится с помощью примитивного многочлена x^2+x+2, α – примитивный элемент. Код БЧХ над полем $GF(3)$ с параметрами $n=8$, $k=3$ порождается многочленом $g(x)=2+x^2+x^3+2x^4+x^5$, $\alpha,\alpha^2,\alpha^3,\alpha^4$ – его подряд идущие корни. На приемном конце получен вектор $v=(0,\ 2,\ 2,\ 2,\ 2,\ 2,\ 0,\ 1)$, в котором не более двух ошибок. Построить поле $GF(3^2)$. Найти соответствующий кодовый вектор u и информационный вектор i.
91. Поле $GF(2^3)$ строится с помощью примитивного многочлена x^3+x+1, α – примитивный элемент. Код Рида-Соломона с параметрами $n=7$, $k=3$, $d=5$ исправляет до двух ошибок. Во всех задачах кодирование и декодирование производить с помощью многочленов Мэттсона-Соломона. В ответах все компоненты векторов записать в виде степеней элемента α (как в заданиях).

- Закодировать информационный вектор $i=(\alpha^2,\ \alpha,\ \alpha^6)$.
- На приемном конце получен вектор $v=(\alpha,\ \alpha,\ \alpha^4,\ 0,\ \alpha^5,\ \alpha^4,\ \alpha^5)$, в котором не более двух ошибок. Найти соответствующий кодовый вектор u с помощью алгоритма Питерсона-Горенстейна-Цирлера и информационный вектор i.
- На приемном конце получен вектор $v=(\alpha^6,\ 1,\ 1,\ 0,\ 1,\ \alpha^4,\ \alpha^6)$, в котором не более двух ошибок. Найти соответствующий кодовый вектор u с помощью алгоритма Евклида и метода Форни, а также информационный вектор i.

Примерные варианты практических заданий по дисциплине «Техническая защита информации»

92. Подготовить к работе детектор поля D 006 и осуществить с его помощью поиск радиозакладки.
93. Подготовить к работе поисковый прибор ST 032 «Пиранья» и осуществить с его помощью поиск радиозакладки (ИМФ-2).
94. Подготовить к работе поисковый прибор ST 032 «Пиранья» и осуществить с его помощью поиск инфракрасного источника (ИМФ-2).
95. Подготовить к работе генератор шума "ГРОМ-ЗИ-4" и продемонстрировать с его помощью зашумление радиоканала.
96. Подготовить к работе прибор виброакустической защиты SI-3010 и продемонстрировать с его помощью защиту речевой информации от утечки по вибрационному и акустическому каналам.
97. Подготовить к работе широкодиапазонный радиоприёмник AR3000A и продемонстрировать навыки настройки его на заранее указанные источники радиоизлучений.

Примерные варианты практических заданий по дисциплине «Организационное и правовое обеспечение информационной безопасности»

98. Разработать вариант сведений ограниченного доступа для выбранного предприятия (организации).

99. Разработать вариант Обязательства (Соглашения) о неразглашении информации ограниченного доступа для выбранного предприятия (организации).
100. Составить проект приказа руководителя предприятия «Об организации работ по обеспечению безопасности персональных данных» для выбранного предприятия.
101. Разработать вариант политики администрирования информационных систем для выбранного предприятия (организации).
102. Разработать вариант политики антивирусной защиты для выбранного предприятия (организации).
103. Разработать вариант политики использования e-mail и доступа к сети Интернет для выбранного предприятия (организации).
104. Разработать вариант политики использования внешних носителей информации для выбранного предприятия (организации).
105. Разработать тезисы выступления перед сотрудниками выбранной организации по доведению требований информационной безопасности.

8. ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Примерные темы для ВКР приведены в фонде оценочных средств государственной итоговой аттестации в пункте 3.3.

Правила оформления ВКР и требования к ней приводятся в учебно-методическом пособии:

Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2017. 40 с.

Критерии оценки ВКР

«Отлично»: тема полностью раскрыта, использовано оптимальное количество источников и литературы, автор продемонстрировал высокий уровень владения исследовательскими методиками. Работа правильно оформлена. Защита прошла успешно, автор содержательно выступил и ответил на поставленные вопросы. График представления работы соблюден.

«Хорошо»: тема в целом раскрыта, однако работа имеет недостатки и ошибки в проведенном исследовании. Защита прошла неубедительно, автор не сумел ответить на ряд вопросов. Есть ошибки в оформлении. Нарушен график представления работы.

«Удовлетворительно»: работа соответствует специальности, однако имеется определенное несоответствие содержания работы заявленной теме; исследуемая проблема в основном раскрыта, но не отличается новизной, теоретической глубиной и аргументированностью; нарушена логика изложения материала, задачи раскрыты не полностью; в работе не в полной мере использованы необходимые для раскрытия темы научная литература, нормативные документы, а также материалы исследований.

Выставление оценки «неудовлетворительно» на защите возможно, если будут установлены грубые нарушения, например, факт прямого плагиата, когда курсовая полностью списана с курсовой «старших товарищей», с какой-либо книги, взята из Интернета или установлен факт ее заказа для написания стороннему лицу. Иными словами, оценка «неудовлетворительно» ставится, если студент на защите пытается выдать чужую работу за свою. Студент, получивший неудовлетворительную оценку, считается имеющим академическую задолженность

Права лиц, не сдавших государственные аттестационные испытания, отражены в пункте 5.7 ДП-2-01-19 Документированной процедуры “Проведение государственной итоговой аттестации по основным профессиональным образовательным программам высшего образования (бакалавриат, специалитет, магистратура)”.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГИА

а) Список рекомендуемой литературы

основная

1. Вентцель Е.С. Теория вероятностей : учебник для втузов. 11-е изд., стер. М. : КНОРУС, 2010. 664 с.
2. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособие для студентов вузов по спец. 075200 "Компьютер. безопасность" и 075500 "Комплексное обеспечение информ. безопасности автоматиз. систем" . М.: Академия. 2005. 144 с.
3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 192 с.
4. Ильин В.А. Математический анализ : учебник для вузов по спец. "Математика", "Прикладная математика", "Информатика": в 2 ч. Ч. 1 / Ильин Владимир Александрович, В. А. Садовничий, Б. Х. Сендов; под ред. А. Н. Тихонова; Моск. гос. ун-т им. М. В. Ломоносова. - 3-е изд., перераб. и доп. -М. : Велби : Проспект, 2007. - 672 с.
5. Ильин В.А. Математический анализ : учебник для вузов по спец. "Математика", "Прикладная математика" и "Информатика": в 2 ч. Ч. 2 / В. А. Ильин, В. А. Садовничий, Б. Х. Сендов; под ред. А. Н.Тихонова; Моск. гос. ун-т им. М. В. Ломоносова. - 2-е изд., перераб. и доп. - М. : Велби : Проспект, 2007. - 368 с.
6. Курош А.Г. Курс высшей алгебры : учебник для вузов по спец. "Математика". 17-е изд., стер. СПб. : Лань, 2008. 432 с.
7. Рацеев С.М. Математические методы защиты информации : электронный учебный курс / С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2018. — URL: http://edu.ulsu.ru/cources/921/interface
8. Соболев А.Н. Физические основы технических средств обеспечения информационной безопасности : учеб. пособие для вузов по спец. 075500 "Комплексное обеспечение информ. безопасности автоматиз. систем" и 075200 "Компьютер. безопасность" / Соболев Анатолий Николаевич, В. М. Кириллов. М. : Гелиос АРВ, 2004. 224 с.
9. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. Москва : Издательство Юрайт, 2019. 312 с. (Серия : Специалист). ISBN 978-5-9916-9043-0. Текст : электронный // ЭБС Юрайт [сайт]. URL: https://biblio-online.ru/bcode/437163
10. Щеглов А.Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. Москва : Издательство Юрайт, 2019. 309 с. (Серия : Бакалавр и магистр. Академический курс). ISBN 978-5-534-04732-5. Текст : электронный // ЭБС Юрайт [сайт]. URL: https://biblio-online.ru/bcode/433715

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":
1.1. Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации". Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798
1.2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801
1.3. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699
2. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:

2.1. ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008. — URL: https://gostexpert.ru/gost/gost-27001-2006
2.2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-34.10-2012
2.3. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-34.11-2012
2.4. ГОСТ Р 52292-2004 Информационная технология. Электронный обмен информацией. Термины и определения. М.: ИПК Издательство стандартов, 2005. — URL: https://gostexpert.ru/gost/gost-52292-2004
2.5. ГОСТ Р 55021-2012 Информационная технология. Руководство по организации и представлению элементов данных при обмене данными. Методы и принципы кодирования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-55021-2012
2.6. ГОСТ Р 7.0.12-2011 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-7.0.12-2011
2.7. ГОСТ Р 7.0.5-2008 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления. М.: Стандартинформ, 2008. — URL: https://gostexpert.ru/gost/gost-7.0.5-2008
2.8. ГОСТ 7.1-2003 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления. М.: Стандартинформ, 2003. — URL: https://gostexpert.ru/gost/gost-7.1-2003
2.9. ГОСТ Р 7.0.5-2008 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления. М.: Стандартинформ, 2008. — URL: https://gostexpert.ru/gost/gost-7.0.5-2008
3. Михеева Е.А. Введение в дискретную математику : учеб. пособие для 1 курса фак. математики, информ. и авиац. технологий. Ч. 2. Ульяновск : УлГУ, 2016. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/248

учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2017. 40 с. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/915
2. Рацеев С. М. Методические указания для самостоятельной работы студентов при подготовке к государственной итоговой аттестации для студентов специальности 10.05.01 «Компьютерная безопасность» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 298 КБ). - Текст : электронный. Режим доступа: http://lib.ulsu.ru/MegaPro/Download/MObject/4683

Согласовано:

Гл. библ-рь ИБ УлГУ	Полина И.Ю.	20.05.2019
должность сотрудника научной библиотеки	ФИО	подпись дата

б) Программное обеспечение

Для образовательного процесса студенту необходимо рабочее место с ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования (Visual Studio.NET/Code::Blocks).

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва , [2019]. - Режим доступа: https://www.biblio-online.ru.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.

1.5. Znanium.com [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	/ 20.05.2019
должность сотрудника УИТиТ	ФИО	подпись	дата

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Помещение 3/317. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций с набором демонстрационного оборудования для обеспечения тематических иллюстраций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 24). Генератор шума для акустического зашумления помещения. Сканирующий радиоприемник АР 3000 А. Широкополосная антенна. Осциллограф АСК 2102. Прибор В6-9 (селективный вольтметр). Генератор НЧ Г3-118. Поисковый прибор ST 032 «Пиранья». Имитатор закладных устройств ИМФ-2. Универсальный акустический излучатель к генератору акустического шума OMS-2000. Универсальный электромагнитный излучатель к генератору акустического шума. Генератор электромагнитного зашумления Гром-ЗИ4. Детектор поля D 006. Экран настенный, мультимедийный проектор. Информационные плакаты. Компьютер, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106 (3 корпус).

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус

Аудитория -24б для проведения лекционных, лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 11 персональных компьютеров, проектор, экран, системы защиты информации: Соболь, Аккорд, Dallas Lock, Secret Net Studio. Сервер Vimark, АПКШ "Континент", Маршрутизаторы Cisco, Система защиты информации ViPNet. 432017, Ульяновская обл, г Ульяновск, ул Набережная реки Свияги, д 106-2 корпус

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

Разработчик _____ / Ганеев С.М. /
подпись ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1	Внесение изменений в п/п а) Список рекомендуемой литературы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 3	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14
2	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 4	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14

Приложение 3

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Вентцель Е.С. Теория вероятностей : учебник для втузов. 11-е изд., стер. М. : КНОРУС, 2010. 664 с.
2. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособие для студентов вузов по спец. 075200 "Компьютер. безопасность" и 075500 "Комплексное обеспечение информ. безопасности автоматиз. систем" . М.: Академия. 2005. 144 с.
3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 192 с.
4. Ильин В.А. Математический анализ : учебник для вузов по спец. "Математика", "Прикладная математика", "Информатика": в 2 ч. Ч. 1 / Ильин Владимир Александрович, В. А. Садовничий, Б. Х. Сендов; под ред. А. Н. Тихонова; Моск. гос. ун-т им. М. В. Ломоносова. - 3-е изд., перераб. и доп. -М. : Велби : Проспект, 2007. - 672 с.
5. Ильин В.А. Математический анализ : учебник для вузов по спец. "Математика", "Прикладная математика" и "Информатика": в 2 ч. Ч. 2 / В. А. Ильин, В. А. Садовничий, Б. Х. Сендов; под ред. А. Н.Тихонова; Моск. гос. ун-т им. М. В. Ломоносова. - 2-е изд., перераб. и доп. - М. : Велби : Проспект, 2007. - 368 с.
6. Курош А.Г. Курс высшей алгебры : учебник для вузов по спец. "Математика". 17-е изд., стер. СПб. : Лань, 2008. 432 с.
7. Рацеев С.М. Математические методы защиты информации : электронный учебный курс / С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2018. — URL: http://edu.ulsu.ru/cources/921/interface
8. Соболев А.Н. Физические основы технических средств обеспечения информационной безопасности : учеб. пособие для вузов по спец. 075500 "Комплексное обеспечение информ. безопасности автоматиз. систем" и 075200 "Компьютер. безопасность" / Соболев Анатолий Николаевич, В. М. Кириллов. М. : Гелиос АРВ, 2004. 224 с.
9. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. Москва : Издательство Юрайт, 2019. 312 с. (Серия : Специалист). ISBN 978-5-9916-9043-0. Текст : электронный // ЭБС Юрайт [сайт]. URL: https://biblio-online.ru/bcode/437163
10. Щеглов А.Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. Москва : Издательство Юрайт, 2019. 309 с. (Серия : Бакалавр и магистр. Академический курс). ISBN 978-5-534-04732-5. Текст : электронный // ЭБС Юрайт [сайт]. URL: https://biblio-online.ru/bcode/433715

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1. Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации". Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798

1.2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801

1.3. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699

2. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:

2.1. ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008. — URL: https://gostexpert.ru/gost/gost-27001-2006
2.2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-34.10-2012
2.3. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-34.11-2012
2.4. ГОСТ Р 52292-2004 Информационная технология. Электронный обмен информацией. Термины и определения. М.: ИПК Издательство стандартов, 2005. — URL: https://gostexpert.ru/gost/gost-52292-2004
2.5. ГОСТ Р 55021-2012 Информационная технология. Руководство по организации и представлению элементов данных при обмене данными. Методы и принципы кодирования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-55021-2012
2.6. ГОСТ Р 7.0.12-2011 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-7.0.12-2011
2.7. ГОСТ Р 7.0.5-2008 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления. М.: Стандартинформ, 2008. — URL: https://gostexpert.ru/gost/gost-7.0.5-2008
2.8. ГОСТ 7.1-2003 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления. М.: Стандартинформ, 2003. — URL: https://gostexpert.ru/gost/gost-7.1-2003
2.9. ГОСТ Р 7.0.5-2008 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления. М.: Стандартинформ, 2008. — URL: https://gostexpert.ru/gost/gost-7.0.5-2008
3. Михеева Е.А. Введение в дискретную математику : учеб. пособие для 1 курса фак. математики, информ. и авиац. технологий. Ч. 2. Ульяновск : УлГУ, 2016. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/248

учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2017. 40 с. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/915
2. Рацеев С. М. Методические указания для самостоятельной работы студентов при подготовке к государственной итоговой аттестации для студентов специальности 10.05.01 «Компьютерная безопасность» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 298 КБ). - Текст : электронный. Режим доступа: http://lib.ulsu.ru/MegaPro/Download/MObject/4683

Согласовано:

Гл. библ-рь ИБ УлГУ	Полина И.Ю.		20.05.2019
должность сотрудника научной библиотеки	ФИО	подпись	дата

Приложение 4

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва , [2019]. - Режим доступа: https://www.biblio-online.ru.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.

1.5. Znanium.com [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	/ 20.05.2019
должность сотрудника УИТиТ	ФИО	подпись	дата