МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (КБГУ)

ИНСТИТУТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЦИФРОВЫХ ТЕХНОЛОГИЙ
КАФЕДРА ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

СОГЛАСОВАНО
Руководитель образовательной программы _____ **А.Р. Бечелова**
«30» 05 **2023г.**

УТВЕРЖДАЮ
Директор института _____ **А.Х. Шапсигов**
«30» 05 **2023г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

02.04.02 Фундаментальная информатика и информационные технологии
(код и наименование направления подготовки)

«**Моделирование систем искусственного интеллекта**»
(наименование профиля подготовки)

Магистр
Квалификация (степень) выпускника

Очная
Форма обучения

Нальчик – 2023

Рабочая программа дисциплины «Математические основы информационной безопасности»/ сост. М.Х. Абрегов - Нальчик: КБГУ, 2023. – 42 с.

Рабочая программа предназначена для преподавания дисциплины «Математические основы информационной безопасности» магистрантам очной формы обучения направления подготовки 02.04.02 – «Фундаментальная информатика и информационные технологии» магистерской программы «Моделирование систем искусственного интеллекта» в 4 семестре 2 года.

Рабочая программа составлена с учётом федерального государственного образовательного стандарта высшего образования по направлению подготовки 02.04.02 – «Фундаментальная информатика и информационные технологии» (уровень магистратуры), утвержденного приказом Министерства образования и науки Российской Федерации от 23 августа 2017 г. N 811 (с изменениями и дополнениями). Редакция с изменениями N 1456 от 26.11.2020 (Зарегистрировано в Минюсте РФ 13 сентября 2017 г. Регистрационный N 48168).

С О Д Е Р Ж А Н И Е

1. Цель и задачи освоения дисциплины (модуля)

Цели освоения дисциплины:

- в получении представления о современной методологии обеспечения информационной безопасности и о роли математических методов и программно-технических средств в обеспечении информационной безопасности

Задачи освоения дисциплины:

-в подготовке к применению методов обеспечения информационной безопасности на этапах проектирования, разработки и эксплуатации сложно организованных программных систем.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Математические основы информационной безопасности» относится к обязательной части Блока 1 «Дисциплины (модули)» основной образовательной программы по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии» магистерской программы «Моделирование систем искусственного интеллекта» и изучается в 4 семестре 2 года.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки:

универсальные (УК):

Коды	Содержание компетенций
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

общепрофессиональных (ОПК):

Коды	Содержание компетенций
ОПК-1	Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий

профессиональных (ПК):

Коды	Содержание компетенции
ПК-7	Способен руководить проектами по созданию, внедрению и использованию одной или нескольких сквозных цифровых субтехнологий искусственного

	интеллекта в прикладных областях

В результате освоения дисциплины обучающийся должен:

Знать:

- математические основы, необходимые для решения задач обеспечения информационной безопасности;
- основные криптографические методы, алгоритмы и протоколы;
- основные положения методологии комплексного подхода к обеспечению информационной безопасности;
- виды угроз ИС и методы обеспечения информационной безопасности;
- типовые математические модели информационно безопасных систем;
- основные программно-технические методы и средства обеспечения информационной безопасности подконтрольных объектов, их роль и место в программной архитектуре компьютерных систем;
- типовые подходы к программной реализации базовых сервисов безопасности в компьютерных системах;
- типовые ошибки программирования, приводящие к уязвимостям компьютерных систем;

Уметь:

- применять математические методы в обеспечении информационной безопасности;
- проводить анализ защищенности информационной системы, разрабатывать модели угроз для информационной системы, проектировать и внедрять систему защиты информации в соответствии с разработанной моделью угроз;
- использовать специализированное программное обеспечение для решения задач информационной безопасности;
- выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС;

Владеть:

понятийным аппаратом информационной безопасности;
- навыками применения современного математического инструментария для решения задач в сфере информационной безопасности;
- методикой построения, анализа и применения математических моделей для оценки степени защищенности информационной системы, качества использованных алгоритмов и технологий;

- навыками применения положений современных нормативных документов и стандартов в области информационной безопасности;

- навыками проведения аудита программного обеспечения на предмет наличия типовых ошибок программирования.

4. Содержание и структура дисциплины (модуля)

Таблица 1. Содержание дисциплины (модуля) «Математические основы информационной безопасности» (перечень оценочных средств и контролируемых компетенций)

№ п/п	Наименование раздела/ темы	Содержание раздела	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	**2**	**3**	**4**	**5**
1.	Основные понятия информационной безопасности	Предмет информационной безопасности. Свойства компьютерной информации, важные с точки зрения информационной безопасности: конфиденциальность, целостность и доступность. Угрозы информационной безопасности. Каналы утечки информации. Неформальная модель нарушителя. Обзор стандартов и нормативно-правовой базы в сфере информационной безопасности.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК
2.	Элементы теории информации и кодирования	Сигналы, данные и методы получения информации. Свойства информации. Количество информации как мера уменьшения неопределенности знаний. Алфавитный подход к вычислению количества информации. Определение вероятности и основные правила вычисления количества информации. Информационная модель Шеннона. Формулы Шеннона и Хартли. Понятие кода. Связь между информационной емкостью и средней длиной кода. Избыточность кодирования. Метод сжатия по Хаффману.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК

		Код Хэмминга		
3.	Математические основы криптографии	Множества и отношения. Бинарные отображения. Основная теорема арифметики. Алгоритм деления в Z. Понятие группы. Изоморфизмы групп. Понятие и свойства колец. Кольцо вычетов. Понятие поля. Поля Галуа. Кольца многочленов. Алгоритм деления в A[X]. Разложение в кольце многочленов. Неприводимые многочлены. Китайская теорема об остатках. Эллиптические кривые.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК
4.	Криптографические методы защиты информации	Понятие симметричных алгоритмов шифрования. Обзор классических симметричных алгоритмов. Моноафавитный шифр. Шифр Гронсфельда. Шифр Плейфейера. Шифр Хилла. Одноразовый блокнот. Перестановочные шифры. Диффузия и коффузия. Схема Файстеля. Обзор современных симметричных алгоритмов шифрования. Шифр DES. Шифр AES. Режимы функционирования блочных шифров. Скремблеры. Виды криптоанализа симметричных алгоритмов. Шифрование с открытым ключом. Алгоритм RSA. Понятие и свойства хэш-функции. Электронная шифровая подпись. Обзор современных отечественных и зарубежных стандартов шифрования и ЭЦП. Понятие криптографического протокола. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана. Атака «человек посередине». Алгоритмы генерации	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК

		псевдослучайных последовательностей.		
5.	Идентификация и аутентификация	Понятия идентификации и аутентификации. Виды аутентификации. Типология протоколов аутентификации. Строгая односторонняя аутентификация на основе случайных чисел. Строгая двусторонняя аутентификация на основе случайных чисел. Аутентификация на основе асимметричного алгоритма. Протокол Kerberos. Механизмы аутентификации при осуществлении подключений. Протокол PPP CHAP. Протокол PPP EAP. Стандарт IEEE 802.1x Аутентификация в защищенных соединениях. Протоколы SSL, TLS, SSH, S-HTTP, SOCKS. Семейство протоколов IPSec.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК
6.	Протоколирование и аудит	Понятие и назначение протоколирования и аудита. Подход к протоколированию в «Оранжевой книге». Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура систем активного аудита.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК
7.	Компьютерные вирусы	Общие сведения о компьютерных вирусах. Структура вируса. Классификации вирусов. Файловые вирусы и макровирусы. Загрузочные вирусы. Сетевые черви. Другие классы вредоносных программ: троянские кони, логические бомбы. Технологии маскировки вирусов. Тенденции современных компьютерных вирусов. Понятие антивируса. Методы обнаружения зараженных файлов. Обзор современных антивирусов.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК

		Развертывание системы антивирусной защиты.		
8.	Средства защиты сети	Межсетевые экраны. Виртуальные частные сети. Системы обнаружения вторжений. Анализ защищенности системы.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК
9.	Средства и методы противодействия угрозам доступности информации	Понятие и основные угрозы доступности информации. Показатели эффективности системы. Коэффициент готовности. Методы обеспечения отказоустойчивости. Нейтрализация отказов. Живучесть. Резервирование. Программное обеспечение промежуточного слоя. Архитектурные принципы обеспечения обслуживаемости. Восстановление после отказов.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК
10.	Основные принципы построения систем защиты	Меры противодействия угрозам безопасности. Принципы построения систем защиты. Понятие и назначение модели безопасности. Модель дискреционного доступа. Модель Белла-ЛаПадулы. Ролевая модель контроля доступа. Системы разграничения доступа	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК
11.	Информационная безопасность с точки зрения технологии программирования	Основные принципы разработки безопасных систем. Основные ошибки программирования. Причины и последствия переполнения буфера. Анализ некоторых программных реализаций сервисов безопасности.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК
12.	Техника и методология атаки	Стратегия злоумышленника. Внешний анализ системы. Сканирование портов. Методы определения программно-аппаратной конфигурации системы и способы противодействия. Системы автоматического сканирования.	УК-1 ОПК-1 ПК-7	ПР, ДЗ, РК

		Использование уязвимостей в программном обеспечении. Эксплойты. Примеры наиболее известных уязвимостей в современных компьютерных системах. Виды популярных атак и средства противодействивя. SQLинъекции. Межсайтовый скриптинг.		

Общая трудоёмкость дисциплины «Математические основы информационной безопасности» составляет 4 зачётные единицы (144 часа).

Таблица 2. Структура дисциплины (модуля) «Математические основы информационной безопасности»

Вид работы	**Трудоемкость часов / зачетных единиц**	
	4 семестр	**всего**
Общая трудоемкость (в часах)	**144**	**144**
Контактная работа (в часах):	**40**	**40**
Лекционные занятия (Л)	10	10
Практические занятия (ПЗ)	30	30
Семинарские занятия (СЗ)	-	-
Лабораторные работы (ЛР)	-	-
Самостоятельная работа (в часах), в том числе контактная работа (вне аудиторная):	**77**	**77**
Расчетно-графическое задание	-	-
Реферат (Р)	-	-
Эссе (Э)	-	-
Контрольная работа (КР)	-	-
Самостоятельное изучение разделов	77	77
Курсовой проект (КП), курсовая работа (КР)	-	-
Подготовка и прохождение промежуточной аттестации	27	27
Вид промежуточной аттестации	**Экзамен**	**Экзамен**

Таблица 3. Лекционные занятия

№ п/п	**Тема**
1.	Основные понятия информационной безопасности
2.	Элементы теории информации и кодирования
3.	Математические основы криптографии
4.	Криптографические методы защиты информации
5.	Идентификация и аутентификация

6.	Протоколирование и аудит
7.	Компьютерные вирусы
8.	Средства защиты сети
9.	. Средства и методы противодействия угрозам доступности информации
10.	Основные принципы построения систем защиты
11.	Информационная безопасность с точки зрения технологии программирования
12.	Техника и методология атаки

Таблица 4. Практические занятия (семинарские занятия)

№ п/п	Тема
1.	Множества и отношения. Бинарные отображения.
2.	современных симметричных алгоритмов шифрования
3.	Принципы построения систем защиты.
4.	Методы определения программно-аппаратной конфигурации системы и способы противодействия
5.	Основные принципы разработки безопасных систем.
6.	Анализ некоторых программных реализаций сервисов безопасности.

Таблица 5. Лабораторные работы по дисциплине (модулю)

№ п/п	Тема
1.	Лабораторные работы по дисциплине не предусмотрены

Таблица 6. Самостоятельное изучение разделов дисциплины (модуля)

№ п/п	Вопросы, выносимые на самостоятельное изучение
1.	Самостоятельное изучение теоретических разделов дисциплины по заданию лектора.
2.	Повторение и углубленное изучение лекционного материала
3.	Решение практических задач и подготовка к практическим занятиям
4.	Подготовка к коллоквиуму и экзамену.

5. Оценочные материалы для текущего и рубежного контроля успеваемости и промежуточной аттестации

Конечными результатами освоения программы дисциплины «Математические основы информационной безопасности» являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы.

В ходе изучения дисциплины предусматриваются *текущий, рубежный контроль и промежуточная аттестация.*

Контрольные мероприятия по дисциплине проводятся в соответствии с Положением о балльно-рейтинговой системе аттестации обучающихся КБГУ. Оценка успеваемости обучающегося осуществляется в ходе текущего и рубежного контроля, а также промежуточной аттестации.

5.1. Оценочные материалы для текущего контроля

Цель текущего контроля – оценка результатов работы в семестре и обеспечение своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающегося. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине.

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины включает: ответы на теоретические вопросы на практическом занятии, решение практических задач и выполнение заданий на практическом занятии, самостоятельное выполнение индивидуальных домашних заданий (например, решение задач) с отчетом (защитой) в установленный срок, написание докладов, рефератов.

Оценка качества подготовки на основании выполненных заданий ведется преподавателем (с обсуждением результатов), баллы начисляются в зависимости от сложности задания.

5.1.1. Вопросы по темам дисциплины «Математические основы информационной безопасности» (контролируемые компетенции УК-1, ОПК-1, ПК-7)

Критерии формирования оценок (оценивания) устного опроса

Устный опрос является одним из основных способов учёта знаний обучающегося по дисциплине «Математические основы информационной безопасности». Развёрнутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения.

В результате устного опроса знания, обучающегося оцениваются по шкале:

Количество баллов	**Критерии оценивания**
5	Обучающийся - полно излагает изученный материал, знает все формулы, применяемые методы и их точность; - понимает материал, может обосновать свои суждения, применить знания при решении практических задач и лабораторных заданий для самостоятельного выполнения; - излагает материал последовательно и правильно с точки зрения норм

	литературного языка.
4	Обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для «5» баллов, но допускает несущественные ошибки, которые сам же исправляет, и некоторые недочёты в последовательности и оформлении излагаемого материала.
3	Обучающийся обнаруживает знание и понимание основного материала по данной теме, но: - излагает материал неполно и допускает неточности в определении понятий, знаний методов, их точности; - не умеет достаточно глубоко и доказательно обосновать свои суждения и применять методы; - излагает материал непоследовательно, допускает ошибки.
2	Обучающийся обнаруживает неполное незнание некоторой части раздела изучаемого материала, допускает ошибки в формулировке и формулах, при оценке точности методов.
1	Обучающийся обнаруживает незнание некоторой части раздела изучаемого материала, допускает существенные ошибки в формулировке и формулах, при оценке точности методов.
0	Обучающийся обнаруживает незнание большей части раздела изучаемого материала, допускает ошибки в формулировке и формулах, при оценке точности методов.

Баллы могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных обучающимся на протяжении занятия.

5.1.2. Оценочные материалы для самостоятельной работы обучающегося (типовые задачи) (контролируемые компетенции УК-1, ОПК-1, ПК-7)

Перечень типовых задач для самостоятельной работы сформирован в соответствии с тематикой практических занятий по дисциплине «Математические основы информационной безопасности».

Типовые тестовые задания по дисциплине

1. Какие из этих утверждений, относящихся к шифру Плейфейра, верны?

а) в основе ключа шифра Плейфейера лежит кодовое слово (или фраза);

б) шифр Плейфейера относится к перестановочным шифрам;

в) единицей шифрования в шифре Плейфейера является биграмма; г) шифр Плейфейера не скрывает полностью статистические особенности исходного текста.

2. Какие предположения включает неформальная модель нарушителя? а) о мотивах нарушителя; б) о категориях лиц, к которым может принадлежать нарушитель; в) о социальном статусе нарушителя; г) о предыдущих атаках, осуществленных нарушителем; д) о времени действия нарушителя.

3. Какие объектамы наиболее подвержены угрозам ИБ в сфере экономики (согласно доктрине информационной безопасности РФ)? а) система государственной статистики; б) информационные ресурсы федеральных органов исполнительной власти и СМИ; в) системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими); г) системы бухгалтерского учета; д) кредитно-финансовая система.
4. Подстановочный алгоритм шифрования — это... а) способ шифрования, при отором каждый символ (или последовательность символов) исходного сообщения заменяются другим символом (или другой последовательностью символов); б) способ шифрования, при котором один и тот же ключ используется и для шифрования и для расшифрования текста; в) способ шифрования, при котором используются два свзяанных ключа: один для шифрования, другой для расшифрования; г) способ шифрования, при котором символы открытого текста изменяют порядок следования в соответствии с правилом, которое определяется ключом
5. В каком из представлений матрицы доступа наиболее просто определить файлы, доступ к которым имеет конкретный пользователь? а) ACL; б) списки полномочий субъектов; в) атрибутные схемы.
6. Каков основной недостаток обнаружения вирусов методом эмуляции программ? а) значительная вероятность ложного срабатывания; б) крайне медленная работа антивируса; в) невозможность обнаружения новых вирусов; г) необходимость трудоемкой ручной настройки антивируса.
7. Расшифруйте текст «ПУЁПЭ» (использован шифр Гронсфельда с ключом 12).
8. Как называется свойство современных симметричных алгоритмов: отсутствие статистической взаимосвязи между ключом и зашифрованным текстом?
9. Зашифруйте сообщение 01011 скремблером 101 с ключом 101
10. Какой метод криптоанализа используется для взлома одного раунда шифрования блочного шифра на основе прослеживания изменений схожести между двумя текстами? а) дифференциальный; б) статистический; в) линейный.
11. Открытым ключом RSA является пара (15, 2). Зашифруйте число 5.
12. Чтобы зашифровать сообщение с помощью асимметричного алгоритма шифрования используются: а) открытый ключ отправителя; б) открытый ключ получателя; в) закрытый ключ отправителя; г) закрытый ключ получателя.
13. Криптографическая стойкость алгоритма RSA основана на: а) математическом аппарате эллиптических кривых; б) произведении двух больших простых чисел; в) сложности

разложения на множители больших чисел; г) сложности дискретного логарифмирования.

14. Какие свойства безопасности могут обеспечиваться посредством ЭЦП? а) конфиденциальность; б) целостность; в) доступность; г) апеллируемость; д) аутентичность.
15. Протокол Диффи-Хеллмана — это: а) протокол аутентификации; б) протокол обмена ключами; в) протокол одновременной подписи; г) протокол групповой подписи; д) протокол голосования.
16. Администратор закрыл для сотрудников организации доступ в Интернет, разрешив лишь пользование электронной почтой. К какому виду мер защиты информации относится данная мера? а) политика безопасности верхнего уровня; б) политика безопасности среднего уровня; в) политика безопасности нижнего уровня; г) принцип минимизации привилегий; д) защита поддерживающей инфраструктуры.
17. Модель безопасности Белла-ЛаПадулы... а) ... устанавливает различные уровни «секретности» объектов и субъектов доступа; б) ... устанавливает набор разрешенных операций доступа для каждой пары «субъектобъект»; в) ... привязывает набор разрешенных действий к роли, которую выполняет пользователь; г) ... запрещает некоторым субъектам определенные виды доступа к некоторым объектам.
18. Какие утверждение о протоколе строгой односторонней аутентификации на основе случайных чисел справедливы? а) в основе протокола лежит симметричный алгоритм шифрования; б) на первом шаге проверяющий В отправляет проверяемому А случайное число; в) на втором шаге проверяемый А отправляет проверяющему В зашифрованное сообщение, содержащее полученное на первом шаге случайное число, а также новое случайное число. г) всего протокол требует отправки двух сообщений.
19. Какому требованию должен удовлетворять пароль для противодействия атаке методом социального инжиниринга? а) пароль не должен быть производным от слов любого естественного языка; б) длина пароля должна составлять 12 и более символов; в) пароль нельзя открывать никому; г) разные сервисы должны защищаться разными паролями; д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т.д.
20. Какие недостатки имеют системы обнаружения вторжений, защищающие сегмент сети? а) высокий процент ложных срабатываний; б) не способны контролировать ситуацию во всей сети; в) неспособны анализировать степень проникновения; г) работа

затруднена при высокой загрузке сети; д) снижается эффективность работы сервера, на котором они установлены.

21. Какие вирусы заражают файлы, дописывая в них свою копию? а) файловые вирусы; б) загрузочные вирусы; в) макровирусы; г) сетевые черви; д) троянские кони.
22. Каким образом проникают в систему сетевые черви? а) по электронной почте; б) любым способом вместе с зараженными ими файлами; в) злоумышленник должен вручную внести вирус в систему; г) через Интернет, используя ошибки в сетевых программах; д) через съемные носители данных при срабатывании автозагрузки с них.
23. Как называется свойство информации, позволяющее достоверно установить ее автора? а) целостность; б) апеллируемость; в) доступность; г) конфиденциальность; д) аутентичность

Методические рекомендации по решению задач

Приступая к решению задач, необходимо внимательно изучить теоретический материал по темам, разобрать приводимые в теоретическом материале каждой темы примеры. При выполнении заданий используются формулы и методы, представленные по каждой теме.

Цель заданий – сформировать навык решения практических прикладных задач, навык оценки точности полученного решения и анализа поведения ошибок.

Критерии формирования оценок по заданиям для самостоятельной работы обучающегося (типовые задачи)

Самостоятельная работа оценивается степенью освоения вопросов для самостоятельного изучения и индивидуальным выполнением заданий к практическим занятиям.

В результате знания обучающегося оцениваются по следующей шкале.

Количество баллов	**Критерии оценивания**
5	Обучающийся показал глубокие знания материала по поставленным вопросам, грамотно, логично его излагает, свободно использует необходимые формулы при решении задач.
4	Обучающийся твердо знает материал, грамотно его излагает, не допускает существенных неточностей в процессе решения задач;
3	Обучающийся имеет знания основного материала по поставленным вопросам, но не усвоил его деталей, допускает отдельные неточности при решении задач.
2	Обучающийся имеет неполное знание и понимание основного материала по поставленным вопросам, не усвоил его деталей, допускает неточности при решении задач.

1	Обучающийся обнаруживает значительнее незнание и понимание основного материала по поставленным вопросам, не усвоил его деталей, допускает существенные неточности при решении задач.
0	Обучающийся допускает грубые ошибки в ответе на поставленные вопросы и при решении задач.

Баллы могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных обучающимся на протяжении занятия.

5.2. Оценочные материалы для рубежного контроля

Рубежный контроль проводится с целью определения качества освоения учебного материала в целом. Рубежный контроль осуществляется по более или менее самостоятельным разделам курса и проводится по окончании изучения материала в заранее установленное время.

В течение семестра проводится *три рубежных контрольных мероприятия по графику.*

В качестве форм рубежного контроля можно использовать тестирование (письменное или компьютерное), проведение коллоквиума или контрольных работ. Выполняемые работы должны храниться на кафедре в течении учебного года и по требованию предоставляться в Управление контроля качества.

На рубежные контрольные мероприятия рекомендуется выносить весь программный материал (все разделы) по дисциплине.

Проведение рейтинговых контрольных мероприятий для инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается адаптированными контрольно-измерительными материалами и соответствующей технологией аттестации.

5.2.1. Оценочные материалы для контрольной работы, коллоквиума (контролируемые компетенции УК-1, ОПК-1, ПК-7)

Оценочные материалы для коллоквиумов приведены в п.5.1.1, а оценочные материалы для контрольной работы – в п.5.1.2.

Типовые вопросы к контрольным работам

Контрольная работа № 1. Задание: используя произвольный язык программирования (для выполнения задания в дисплейных классах рекомендуется язык Java), написать программу, осуществляющую шифрование и дешифрование произвольного текста в соответствии с заданным алгоритмом шифрования. Минимальные возможности программы: загрузка и сохранение в файле шифруемого/дешифруемого текста и

результата, загрузка и сохранение в файле ключа. Реализовать наглядное представление ключа в таких алгоримах как решетка Флейберга, шифр Плейфейера. Реализовать проверку допустимости ключа в таких алгоритмах как шифр Гронсфельда.

Варианты контрольной работы:

1) Шифр Гронсфельда
2) Шифр Бэкона
3) Перестановочный шифр
4) Шифр Тритемиуса
5) Шифр Плейфейера
6) Шифр простой замены
7) Квадратичная решетка
8) Шифр Хилла
9) Шифр Вернама
10) Скремблирующая последовательность на основе линейного генератора случайных чисел
11) Скремблирующая последовательность на основе квадратичного генератора случайных чисел.

Контрольная работа № 2. Задание: используя произвольный язык программирования (для выполнения задания в дисплейных классах рекомендуется язык Java), написать программу, реализующую заданный криптографический протокол. Минимальные требования к программе: графический интерфейс пользователя, сетевое взаимодействие участников протокола, клиент для имитации атаки «человек посередине».

Варианты контрольной работы:

1) Строгая односторонняя аутентификация на основе случайных чисел;
2) Строгая двусторонняя аутентификация на основе случайных чисел;
3) Протокол Диффи-Хеллмана
4) Протокол одновременной подписи
5) Протокол групповой подписи
6) Протокол голосования
7) Протокол электронной цифровой подписи (использовать сторонние реализации функций хэширования и асимметричного шифрования).
8) Аутентификация на основе асимметричного алгоритма (использовать стороннюю реализации функций хэширования и асимметричного шифрования).

Контрольная работа № 3.

Задание: студент получает адрес сайта некоторой организации. Используя открытые информационные источники, необходимо проанализировать деятельность этой организации и составить модель угроз для заданной организации, а затем, на основе модели угроз разработать политику безопасности.

Варианты контрольной работы (виды организаций, конкретные адреса сайтов могут меняться):

1) Университет;
2) Министерство субъекта федерации;
3) Интернет-магазин;
4) Библиотека;
5) Производственное предприятие;
6) Редакция;
7) Банк;
8) Страховая компания;
9) Ломбард;
10) Инвестиционный фонд;
11) Адвокатский кабинет;
12) Транспортная компания.

Контрольная работа № 4. Комплексный анализ защищенности информационной системы организации. Студенты получают индивидуальные образы виртуальной машины с установленной и настроенной информационной системой некоторой организации. Задача: смонтировать виртуальный образ, запустить и проанализировать его. Выявить потенциальные уязвимости системы, устранить возможные проблемы безопасности, используя репозиторий свободного программного обеспечения, разработать рекомендации по приобретению необходимого оборудования и ПО (а также их настройке) для ликвидации остальных угроз

Критерии формирования оценок по контрольным точкам (контрольные работы; коллоквиум) Текущий и рубежный контроль

Семестр	**Шкала оценивания**			
	0-35 баллов	**36-50 баллов**	**51-60 баллов**	**56-70 баллов**
4	Частичное посещение аудиторных занятий. Неудовлетворительное выполнение практических работ. Плохая подготовка к	Полное или частичное посещение аудиторных занятий. Частичное выполнение и защита практических работ.	Полное или частичное посещение аудиторных занятий. Полное	Полное посещение аудиторных занятий. Полное выполнение и

	балльно-рейтинговым мероприятиям. Обучающийся не допускается к промежуточной аттестации	Выполнение контрольных работ, ответы на коллоквиуме на оценки «удовлетворительно».	выполнение и защита практических работ. Выполнение контрольных работ, ответы на коллоквиуме на оценки «хорошо».	защита практических занятий. Выполнение контрольных работ, ответы на коллоквиуме на оценки «отлично».

5.2.2. Оценочные материалы для промежуточной аттестации (контролируемые компетенции УК-1, ОПК-1, ПК-7)

Целью промежуточной аттестации по дисциплине «Математические основы информационной безопасности» является оценка качества освоения дисциплины обучающимися.

Промежуточная аттестация предназначена для объективного подтверждения и оценивания достигнутых результатов обучения после завершения изучения дисциплины.

Промежуточная аттестация осуществляется в конце семестра и представляет собой итоговую оценку знаний по дисциплине в форме проведения экзамена, которым заканчивается изучение дисциплины. Он может проводиться в устной и письменной форме. Устный опрос является одним из основных способов учёта знаний обучающегося по данной дисциплине.

Для допуска к экзамену, обучающемуся необходимо иметь не менее 36 баллов.

Вопросы, выносимые на экзамен по дисциплине «Математические основы информационной безопасности» (контролируемые компетенции УК-1, ОПК-1, ПК-7)

1. Свойства компьютерной информации, важные с точки зрения информационной безопасности: конфиденциальность, целостность и доступность.
2. Угрозы информационной безопасности.
3. Каналы утечки информации.
4. Неформальная модель нарушителя.
5. Обзор стандартов и нормативно-правовой базы в сфере информационной безопасности.
6. Сигналы, данные и методы получения информации. Свойства информации.
7. Количество информации как мера уменьшения неопределенности знаний. Алфавитный подход к вычислению количества информации.
8. Определение вероятности и основные правила вычисления количества информации.

9. Информационная модель Шеннона.
10. Формулы Шеннона и Хартли.
11. Понятие кода. Связь между информационной емкостью и средней длиной кода. Избыточность кодирования.
12. Метод сжатия по Хаффману.
13. Код Хэмминга
14. Множества и отношения. Бинарные отображения.
15. Основная теорема арифметики. Алгоритм деления в Z.
16. Понятие группы. Изоморфизмы групп.
17. Понятие и свойства колец. Кольцо вычетов.
18. Понятие поля. Поля Галуа.
19. Кольца многочленов. Алгоритм деления в A[X]. Разложение в кольце многочленов. Неприводимые многочлены.
20. Китайская теорема об остатках
21. Эллиптические кривые.
22. Понятие симметричных алгоритмов шифрования.
23. Обзор классических симметричных алгоритмов. Моноафавитный шифр. Шифр Гронсфельда. Шифр Плейфейера. Шифр Хилла. Одноразовый блокнот. Перестановочные шифры.
24. Диффузия и коффузия. Схема Файстеля.
25. Обзор современных симметричных алгоритмов шифрования. Шифр DES. Шифр AES.
26. Режимы функционирования блочных шифров.
27. Скремблеры.
28. Виды криптоанализа симметричных алгоритмов.
29. Шифрование с открытым ключом. Алгоритм RSA.
30. Понятие и свойства хэш-функции.
31. Электронная шифровая подпись.
32. Обзор современных отечественных и зарубежных стандартов шифрования и ЭЦП.
33. Понятие криптографического протокола.
34. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана. Атака «человек посередине».
35. Алгоритмы генерации псевдослучайных последовательностей.
36. Понятия идентификации и аутентификации. Виды аутентификации. Типология протоколов аутентификации.

37. Строгая односторонняя аутентификация на основе случайных чисел. Строгая двусторонняя аутентификация на основе случайных чисел. Аутентификация на основе асимметричного алгоритма.
38. Протокол Kerberos.
39. Механизмы аутентификации при осуществлении подключений. Протокол PPP CHAP. Протокол PPP EAP. Стандарт IEEE 802.1x
40. Аутентификация в защищенных соединениях. Протоколы SSL, TLS, SSH, S-HTTP, SOCKS. Семейство протоколов IPSec.
41. Понятие и назначение протоколирования и аудита. Подход к протоколированию в «Оранжевой книге».
42. Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура систем активного аудита.
43. Общие сведения о компьютерных вирусах. Структура вируса. Классификации вирусов.
44. Файловые вирусы и макровирусы. Загрузочные вирусы. Сетевые черви. Другие классы вредоносных программ: троянские кони, логические бомбы.
45. Технологии маскировки вирусов. Тенденции современных компьютерных вирусов.
46. Понятие антивируса. Методы обнаружения зараженных файлов. Обзор современных антивирусов.
47. Развертывание системы антивирусной защиты.
48. Межсетевые экраны.
49. Виртуальные частные сети.
50. Системы обнаружения вторжений. Анализ защищенности системы.
51. Понятие и основные угрозы доступности информации. Показатели эффективности системы. Коэффициент готовности.
52. Методы обеспечения отказоустойчивости. Нейтрализация отказов. Живучесть. Резервирование. Программное обеспечение промежуточного слоя.
53. Архитектурные принципы обеспечения обслуживаемости. Восстановление после отказов.
54. Меры противодействия угрозам безопасности.
55. Принципы построения систем защиты.
56. Понятие и назначение модели безопасности.
57. Модель дискреционного доступа. Модель Белла-ЛаПадулы. Ролевая модель контроля доступа.

58. Системы разграничения доступа
59. Основные принципы разработки безопасных систем.
60. Основные ошибки программирования. Причины и последствия переполнения буфера.
61. Анализ некоторых программных реализаций сервисов безопасности.
62. Стратегия злоумышленника.
63. Использование уязвимостей в программном обеспечении.
64. SQL-инъекции.
65. Межсайтовый скриптинг

Критерии формирования оценок по промежуточной аттестации (для экзамена в случае, если экзаменационный билет содержит два вопроса)

Семестр	**Шкала оценивания** *(по итогам текущего и рубежного контроля)*			
	Неудовлетворит. (36-60 баллов)	**Удовлетворит. (61-80 баллов)**	**Хорошо (81-90 баллов)**	**Отлично (91-100 баллов)**
4	Обучающийся имеет 36-60 баллов по итогам текущего и рубежного контроля, на экзамене не дал полного ответа ни на один вопрос. Обучающийся имеет 36-45 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ только на один вопрос	Обучающийся имеет 36-50 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос и частично (полностью) ответил на второй. Обучающийся имеет 46-60 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос или частично ответил на оба вопроса. Обучающийся имеет по итогам текущего и рубежного контроля 61-70 баллов на экзамене не дал полного ответа ни	Обучающийся имеет 51-60 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос и частично (полностью) ответил на второй. Обучающийся имеет 61 – 65 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос и частично ответил на второй. Обучающийся имеет 66-70 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ только на один	Обучающийся имеет 61-70 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос и частично (полностью) ответил на второй.

		на один вопрос	вопрос.	

6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Учебная работа по дисциплине состоит из контактной работы (лекции, практические занятия) и самостоятельной работы.

Максимальная сумма (100 баллов), набираемая обучающимся по дисциплине включает две составляющие:

– *первая составляющая* – оценка регулярности, своевременности и качества выполнения обучающимся учебной работы по изучению дисциплины в течение периода изучения дисциплины (семестра, или нескольких семестров) (сумма – не более 70 баллов). Баллы, характеризующие успеваемость обучающегося по дисциплине, набираются им в течение всего периода обучения за изучение отдельных тем и выполнение отдельных видов работ.

– *вторая составляющая* – оценка знаний обучающегося по результатам промежуточной аттестации (не более 30 –баллов).

Общий балл текущего и рубежного контроля складывается из следующих составляющих:

Критерии оценки качества освоения дисциплины

Оценка «отлично»– от 91 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене обучающийся демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка «хорошо» – от 81 до 90 баллов – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене обучающийся демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «удовлетворительно» – от 61 до 80 баллов – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене

обучающийся демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

Оценка «неудовлетворительно» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене обучающийся демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины.

Распределение баллов текущего и рубежного контроля

№ п/п	Вид контроля	Сумма баллов			
		Общая сумма в баллах	**1-я точка**	**2-я точка**	**3-я точка**
1.	**Посещение занятий**	**10**	**3**	**3**	**4**
2.	**Текущий контроль:**	**до 30**	**до 10**	**до 10**	**до 10**
	Выполнение самостоятельных заданий (решение задач)	0 -15	0 - 5	0 -5	0 - 5
3.	**Рубежный контроль**	**до 30**	**до 10**	**до 10**	**до 10**
	тестирование	0- 12	0- 4	0- 4.	0- 4.
	коллоквиум	0 - 18	0 - 6	0 -6	0 - 6
4.	**Итого сумма текущего и рубежного контроля**	**до 70**	**до 23**	**до 23**	**до 24**
	Первый этап (базовый уровень) – оценка «удовлетворительно»	не менее 36	не менее 12	не менее 12	не менее 12
	Второй этап (продвинутый уровень) – оценка «хорошо»	менее 70 (51-69)	менее 23	менее 23	менее 24
	Третий этап (высокий уровень) - оценка «отлично»	не менее 70	не менее 23	не менее 23	не менее 24

Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися.

Проводится комплексная проверка обучающихся на определение степени овладения знаниями, умениями и навыками, полученными на занятиях, а также путём самостоятельной работы.

Типовые задания, обеспечивающие формирование компетенций представлены в таблице 7.

Таблица 7. Результаты освоения учебной дисциплины, подлежащие проверке

Результаты обучения (компетенции)	**Индикаторы достижения компетенций**	**Вид оценочного материала, обеспечивающий формирование компетенций**	**Основные показатели оценки результатов обучения**
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**УК-1.5.** Проводит поиск зарегистрированных результатов интеллектуальной деятельности и средств индивидуализации при создании инновационных продуктов в профессиональной деятельности	Типовые оценочные материалы для устного опроса (п. 5.1.1); типовые оценочные материалы для контрольной работы (п. 5.1.2); типовые оценочные материалы к экзамену (п. 5.2.2)	УК-1.5. З-1. Знает методы выполнения поиска зарегистрированных результатов интеллектуальной деятельности и средств индивидуализации УК-1.5. У-1. Умеет применять методы исследований результатов интеллектуальной деятельности и средств индивидуализации при создании инновационных продуктов в профессиональной деятельности
ОПК-1. Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальных информатики и информационных технологий	**ОПК-1.1.** Применяет инструментальные среды, программно-технические платформы для решения задач в области создания и применения искусственного интеллекта	Типовые оценочные материалы для устного опроса (п. 5.1.1); типовые оценочные материалы для контрольной работы (п. 5.1.2); типовые оценочные материалы к экзамену (п. 5.2.2)	ОПК-1.1. З-1. Знает инструментальные среды, программно-технические платформы для решения профессиональных задач ОПК-1.1. У-1. Умеет применять инструментальные среды, программно-технические платформы для решения профессиональных задач
ПК-7. Способен руководить проектами по созданию, внедрению и использованию	**ПК-7.3.** Руководит проектами в области сквозной цифровой субтехнологии «Рекомендательные системы и системы	Типовые оценочные материалы для устного опроса (п. 5.1.1); типовые оценочные материалы для	ПК-7.3. З-1. Знает фундаментальные правила построения рекомендательных систем и систем поддержки принятия

одной или нескольких сквозных цифровых субтехнологий искусственного интеллекта в прикладных областях	поддержки принятия решений»	контрольной работы (п. 5.1.2); типовые оценочные материалы к экзамену (п. 5.2.2)	решений, основанных на интеллектуальных принципах, методы и подходы к планированию и реализации проектов по созданию систем искусственного интеллекта на основе сквозной цифровой субтехнологии «Рекомендательные системы и системы поддержки принятия решений» ПК-7.3. У-1. Умеет руководить проектами по созданию, внедрению и поддержке систем искусственного интеллекта на основе сквозной цифровой субтехнологии «Рекомендательные системы и системы поддержки принятия решений»

7. Учебно-методическое обеспечение дисциплины

7.1. Нормативно-законодательные акты

1. Приказ Минобрнауки России от 05.04.2017 №301 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры" (Зарегистрировано в Минюсте России 14.07.2017 № 47415).
2. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 02.04.02 – «Фундаментальная информатика и информационные технологии» (уровень магистратуры), утвержденный приказом Министерства образования и науки Российской Федерации от 23 августа 2017 г. N 811 (Зарегистрировано в Минюсте РФ 13 сентября 2017 г. Регистрационный N 48168) (с изм. и доп., вступ. в силу с 01.09.2021).
3. Федеральный закон "Об образовании в Российской Федерации" от 29.12.2012 N 273-ФЗ http://www.consultant.ru/document/cons_doc_LAW_140174/

7.2. Основная литература

1. Ярочкин В.И. Информационная безопасность [Текст]: учеб. для студентов вузов, обучающихся по гуманитар. и социал.-экон. специальностям / В. И. Ярочкин. - М.: Гаудеамус: Акад. Проект, 2008.
2. Информационная безопасность и защита информации [Текст]: учеб. пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 4-е изд., стер. - М.: Изд. центр "Академия", 2009.
3. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / Башлы П. Н. – Москва: Евразийский открытый институт, 2012. -311 c. 978-5-374-00301-7 Книга находится в базовой версии ЭВС IPRbooks/

7.3. Дополнительная литература

1. Конеев И.Р. Информационная безопасность предприятия [Текст]: [учеб. пособие] / И. Р. Конеев, А. В. Беляев. - СПб.: БХВ-Петербург, 2003.
2. Криптография на Си и C++ в действии [Текст]: учеб. пособие / М. Вельшенбах. - М.: Триумф, 2004.
3. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004 г.
4. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]: учеб. пособие / А. А. Малюк. - М.: Горячая линия - Телеком, 2004.
5. Смарт Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. - М: Техносфера, 2006.
6. Шнайер Брюс. Секреты и ложь. Безопасность данных в цифровом мире. СПб.: Питер, 2003.
7. Реализация численных методов в среде Matlab (в 2-х частях). Лабораторный практикум. Бештоков М.Х., Тхамоков М.Б., Хамова М.З. Электр. Ресурс. КБГУ, Нальчик, 2013. (60 экз.)

7.4. Периодические издания

1. Искусственный интеллект и принятие решений – журнал URL: http://aidt.ru
2. Информационно-управляющие системы - журнал URL: http://www.i-us.ru
3. Открытые системы – информационный портал; URL: http://www.olap.ru/basic/refer.asp.
4. Системы управления и информационные технологии – журнал, URL: http://www.sbook.ru/suit/

7.5. Интернет-ресурсы

1. Портал по информационной безопасности http://www.securitylab.ru/
2. Учебные ресурсы центра «Новые информационные технологии» http://nto.immpu.sgu.ru

При проведении занятий лекционного типа практических (семинарских) занятий используются сведения об электронных информационных ресурсах, к которым обеспечен доступ для пользователей библиотеки КБГУ.

Перечень актуальных электронных информационных баз данных, к которым обеспечен доступ пользователям КБГУ (2023-2024 уч. год)

№ п/п	Наименование электронного ресурса	Краткая характеристика	Адрес сайта	Наименование организации-владельца; реквизиты договора	Условия доступа
1.	**Научная электронная библиотека (НЭБ РФФИ)**	Электр. библиотека научных публикаций - около 4000 иностранных и 3900 отечественных научных журналов, рефераты публикаций 20 тыс. журналов, а также описания 1,5 млн. зарубежных и российских диссертаций; 2800 росс. журналов на безвозмездной основе	http://elibrary.ru	ООО «НЭБ» Лицензионное соглашение №14830 от 01.08.2014г. Бессрочное	Полный доступ
2.	**ЭБС «Консультант студента»**	13800 изданий по всем областям знаний, включает более чем 12000 учебников и учебных пособий для ВО и СПО, 864 наименований журналов и 917 монографий.	http://www.studmedlib.ru http://www.medcollegelib.ru	ООО «Консультант студента» (г. Москва) **Договор №750КС/07-2022** От 26.09.2022 г. Активен до 30.09.2023г.	Полный доступ (регистрация по IP-адресам КБГУ)

3.	**«Электронная библиотека технического вуза» (ЭБС «Консультант студента»)**	Коллекция «Медицина (ВО) ГЭОТАР-Медиа. Books in English (книги на английском языке)»	http://www.studmedlib.ru	ООО «Политехресурс» (г. Москва) **Договор №849КС/03-2023** от 11.04.2023 г. Активен до 19.04.2024г.	Полный доступ (регистрация по IP-адресам КБГУ)
4.	**ЭБС «Лань»**	Электронные версии книг ведущих издательств учебной и научной литературы (в том числе университетских издательств), так и электронные версии периодических изданий по различным областям знаний.	https://e.lanbook.com/	ООО «ЭБС ЛАНЬ» (г. Санкт-Петербург) **Договор №41ЕП/223** от 14.02.2023 г. Активен до 15.02.2024г.	Полный доступ (регистрация по IP-адресам КБГУ)
5.	**ЭБС «Лань»**	Коллекция электронных изданий «ФПУ. 10-11 кл. Изд-во «Просвещение». Общеобразовательные предметы.	https://e.lanbook.com/	ООО «ЭБС ЛАНЬ» (г. Санкт-Петербург) **Договор №246ЕП/223** от 31.07.2023 г. Активен до 01.09.2024г.	Полный доступ (регистрация по IP-адресам КБГУ)
6.	**Национальная электронная библиотека РГБ**	Объединенный электронный каталог фондов российских библиотек, содержащий 4 331 542 электронных документов образовательного и научного характера по различным отраслям знаний	https://rusneb.ru/	ФГБУ «Российская государственная библиотека» Договор №101/НЭБ/1666-п от 10.09.2020г. Бессрочный	Доступ с электронного читального зала библиотеки КБГУ
7.	**ЭБС «IPSMART»**	107831 публикаций, в т.ч.: 19071 – учебных изданий, 6746 – научных изданий,	http://iprbookshop.ru/	ООО «Ай Пи Эр Медиа» (г. Москва) **Договор №75/ЕП-223**	Полный доступ (регистрация по IP-адресам КБГУ)

		700 коллекций, 343 журнала ВАК, 2085 аудиоизданий.		от 23.03.2023 г. Активен до 02.04.2024г.	
8.	**ЭБС «IPSMART» (ЭОР РКИ)**	Тематическая коллекция «Русский язык как иностранный» Издательские коллекции: «Златоуст»; «Русский язык. Курсы»; «Русский язык» (Курсы УМК «Русский язык сегодня» - 6 книг)	http://iprbookshop.ru/ http://www.ros-edu.ru/	ООО «Ай Пи Эр Медиа» (г. Москва) **Договор №142/ЕП-223** от 18.05.2023 г. срок предоставления лицензии: с 01.06.2023 по 01.06.2024	Полный доступ (регистрация по IP-адресам КБГУ)
9.	**ЭБС «Юрайт» для СПО**	Электронные версии учебной и научной литературы издательств «Юрайт» для СПО и электронные версии периодических изданий по различным областям знаний.	https://urait.ru/	ООО «Электронное издательство ЮРАЙТ» (г. Москва) **Договор №305/ЕП-223** От 27.10.2022 г. Активен до 31.10.2023 г.	Полный доступ (регистрация по IP-адресам КБГУ)
10.	**ЭБС «Юрайт» для ВО**	Электронные версии 8000 наименований учебной и научной литературы издательств «Юрайт» для ВО и электронные версии периодических изданий по различным областям знаний.	https://urait.ru/	ООО «Электронное издательство ЮРАЙТ» (г. Москва) **Договор №44/ЕП-223** От 16.02.2023 г. Активен с 01.03.2023 г. по 29.02.2024 г.	Полный доступ (регистрация по IP-адресам КБГУ)
11.	**Polpred.com. Новости. Обзор СМИ. Россия и зарубежье**	Обзор СМИ России и зарубежья. Полные тексты + аналитика из 600 изданий по 53 отраслям	http://polpred.com	ООО «Полпред справочники» Безвозмездно (без официального договора)	Доступ по IP-адресам КБГУ
12.	**Президентская**	Более 500 000	http://www.prlib	ФГБУ	Авторизованн

	библиотека им. Б.Н. Ельцина	электронных документов по истории Отечества, российской государственности, русскому языку и праву	.ru	«Президентская библиотека им. Б.Н. Ельцина» (г. Санкт-Петербург) **Соглашение от 15.11.2016г**. Бессрочный	ый доступ из библиотеки (ауд. №115, 214)

7.6. Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы

Учебная работа по дисциплине «Математические основы информационной безопасности» состоит из контактной работы (лекции, практические занятия) и самостоятельной работы.

Цель курса - подготовка обучающихся к научно-исследовательской деятельности в области прикладной математики, к умению применять полученные знания к решению прикладных задач математической физики. Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться с тематическим планом занятий, списком рекомендованной учебной литературы. При изучении дисциплины, обучающиеся выполняют следующие задания: изучают рекомендованную учебную и научную литературу; пишут контрольные работы, готовят сообщения к практическим занятиям; выполняют самостоятельные работы, участвуют в выполнении практических заданий. Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях, изучения рекомендованной литературы, выполнения контрольных письменных заданий

Курс изучается на лекциях, при самостоятельной и индивидуальной работе обучающихся. Обучающийся для полного освоения материала должен не пропускать занятия и активно участвовать в учебном процессе. Лекции включают все темы и основные вопросы теории и практики. Для максимальной эффективности изучения необходимо постоянно вести конспект лекций, знать рекомендуемую преподавателем литературу, позволяющую дополнить знания и лучше подготовиться к практическим занятиям.

В соответствии с учебным планом на каждую тему выделено необходимое количество часов практических занятий, которые проводятся в соответствии с вопросами, рекомендованными к изучению по определенным темам. Обучающиеся должны регулярно готовиться к практическим занятиям и участвовать в обсуждении вопросов.

При подготовке к занятиям следует руководствоваться конспектом лекций и рекомендованной литературой. Тематический план дисциплины, учебно-методические материалы, а также список рекомендованной литературы приведены в рабочей программе.

Методические рекомендации при работе над конспектом во время проведения лекции

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются общие и утвердившиеся в практике правила, и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Целесообразно записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому обучающемуся необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

Методические рекомендации по подготовке к практическим занятиям

Практические (семинарские) занятия – составная часть учебного процесса, групповая форма занятий при активном участии обучающихся. Практические занятия способствуют углубленному изучению наиболее сложных проблем науки и служат основной формой подведения итогов самостоятельной работы обучающихся.

Целью практических занятий является углубление и закрепление теоретических знаний, полученных обучающимися на лекциях и в процессе самостоятельного изучения учебного материала, следовательно, формирование у них определенных умений и навыков.

Желательно при подготовке к практическим занятиям по дисциплине одновременно использовать несколько источников, раскрывающих заданные вопросы.

На практических занятиях обучающиеся учатся грамотно излагать проблемы, свободно высказывать свои мысли и суждения, рассматривают ситуации,

способствующие развитию профессиональной компетентности. Следует иметь в виду, что подготовка к практическому занятию зависит от формы, места проведения семинара, конкретных заданий и поручений.

Для подготовки к практическим занятиям необходимо рассмотреть контрольные вопросы, при необходимости обратиться к рекомендуемой литературе, записать непонятные моменты в вопросах для уяснения их на предстоящем занятии.

Методические рекомендации по организации самостоятельной работы

Для самостоятельной работы имеются помещения, оснащённые компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную библиотеку. Имеется электронный вариант конспекта лекций,

Самостоятельная работа обучающихся – способ активного, целенаправленного приобретения обучающимся новых для него знаний и умений без непосредственного участия в этом процесса преподавателей. Повышение роли самостоятельной работы обучающихся при проведении различных видов учебных занятий предполагает:

- оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование информационных технологий, позволяющих обучающемуся в удобное для него время осваивать учебный материал;

- широкое внедрение компьютеризированного тестирования;

- совершенствование методики проведения практик и научно-исследовательской работы обучающихся, поскольку именно эти виды учебной работы в первую очередь готовят обучающихся к самостоятельному выполнению профессиональных задач;

- модернизацию системы курсового и дипломного проектирования, которая должна повышать роль обучающегося в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит обучающегося к получению новых знаний, упорядочению и углублению имеющихся знаний, формированию профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций:

- развивающую;
- информационно-обучающую;
- ориентирующую и стимулирующую;
- воспитывающую;
- исследовательскую.

В рамках курса выполняются следующие виды самостоятельной работы:

1) проработка учебного материала (по конспектам, учебной и научной литературе);

2) выполнение разно уровневых задач и заданий;

3) работа с тестами и вопросами для самопроверки;

4) выполнение итоговой контрольной работы.

Обучающемуся рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые обучающийся получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса обучающийся может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций и лабораторный практикум. Он же может использоваться и для закрепления полученного в аудитории материала.

Самостоятельная работа обучающихся предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости обучающийся может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач. Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее обучающимся и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю

достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать вычислительные задачи и получать знания. Использование сетей усиливает роль самостоятельной работы обучающегося и позволяет кардинальным образом изменить методику преподавания.

Обучающийся может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Обучающийся имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде обучающегося имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет обучающемуся своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений. Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий – это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

Методические рекомендации по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой необходимо учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность обучающемуся сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов обучающийся будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в ФОС в перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью *изучающего* чтения является глубокое и всестороннее понимание учебной информации. Есть несколько приемов изучающего чтения:

- чтение по алгоритму предполагает разбиение информации на блоки: название, автор, источник, основная идея текста, фактический материал, анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам, новизна;

- прием постановки вопросов к тексту имеет следующий алгоритм: медленно прочитать текст, стараясь понять смысл изложенного; выделить ключевые слова в тексте; постараться понять основные идеи, подтекст и общий замысел автора.

- прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

Можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Подготовка к экзамену должна проводиться на основе лекционного материала, материала практических занятий с обязательным обращением к основным учебникам по курсу. Это позволит исключить ошибки в понимании материала, облегчит его осмысление, прокомментирует материал многочисленными примерами.

Методические рекомендации для подготовки к экзамену

Экзамен в 4 семестре является формой итогового контроля знаний и умений, обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в

процессе самостоятельной работы. Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

К экзамену допускаются обучающиеся, набравшие 36 и более баллов по итогам текущего и промежуточного контроля. На экзамене обучающийся может набрать от 15 до 30 баллов.

В период подготовки к экзамену обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка обучающегося к экзамену включает три этапа:

– самостоятельная работа в течение семестра;
– непосредственная подготовка в дни, предшествующие экзамену по темам курса;
– подготовка к ответу на экзаменационные вопросы.

При подготовке к экзамену обучающимся целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На экзамен выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Экзамен проводится в письменной / устной форме.

При проведении экзамена в письменной (устной) форме, ведущий преподаватель составляет экзаменационные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня экзаменационных вопросов, доведенных до сведения обучающихся накануне экзаменационной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится устный экзамен, должно одновременно находиться не более шести обучающихся на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 40 минут.

При проведении письменного экзамена на работу отводится 60 минут.

Результат устного (письменного) экзамена выражается оценками:

Оценка «отлично»– от 91 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене обучающийся демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка «хорошо» – от 81 до 90 баллов – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене обучающийся демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «удовлетворительно» – от 61 до 80 баллов – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене обучающийся демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

Оценка «неудовлетворительно» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене обучающийся демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины**.**

8. Материально-техническое обеспечение дисциплины

8.1. Требования к материально-техническому обеспечению

Для реализации рабочей программы дисциплины «Интеллектуальный анализ данных» имеются специальные помещения для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы. Специальные помещения укомплектованы специализированной мебелью и техническими средства обучения, служащими для представления информации большой аудитории.

Для проведения занятий лекционного типа используется демонстрационное оборудование, позволяющее наиболее эффективно освоить представленный учебный материал.

При проведении занятий лекционного/ семинарского типа занятий используются:

№ п/п	Наименование программы, право использования которой предоставляется	Страна происхождения	Срок действия программного обеспечения	Кол-во

1.	*Операционная система РЕД ОС. Конфигурация: «Рабочая станция»*	Российская Федерация	12 месяцев	1000
2.	Система оптического распознавания текста *SETERE OCR для РЭД ОС*	Российская Федерация	12 месяцев	30
3.	Лицензия на программное обеспечение средств антивирусной защиты *Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition*	Российская Федерация	12 месяцев	700
4.	Право использования программного обеспечения для планирования и проведения онлайн-мероприятий (трансляций, телемостов/ аудио-видеоконференций, вебинаров) *Webinar Enterprise TOTAL 150 участников*	Российская Федерация	12 месяцев	1
5.	Лицензия на программное обеспечение для векторного графического редактора для создания и редактирования графических схем, чертежей и блок-схем *Асмо-графический редактор*	Российская Федерация	бессрочные	32
6.	Предоставление неисключительных прав на использование программного обеспечения Системы *Spider Project Professional*	Российская Федерация	бессрочные	16

8.2. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для обучающихся с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;

2. Для инвалидов с нарушениями зрения (слабовидящие, слепые)

- присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники,

видеоувеличителей, программ невизуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для обучающихся с нарушениями зрения;

- задания для выполнения на экзамене зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;

3. Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):

- на зачете присутствует ассистент, оказывающий обучающемуся необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- зачет проводится в письменной форме;

4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия, обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекту питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений);

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию обучающегося экзамен проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

9. Лист изменений (дополнений)

в рабочей программе дисциплины «Математические основы информационной безопасности» направления подготовки 02.04.02 – Фундаментальная информатика и информационные технологии магистерской программы «Моделирование систем искусственного интеллекта» на 2023-2024 учебный год.

№ п/п	Элемент (пункт) РПД	Перечень вносимых изменений (дополнений)	Примечание
1.			
2.			
3.			