

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет компьютерных технологий и прикладной математики

УТВЕРЖДАЮ

Проректор по учебной работе,
качеству образования – первый
проректор

Хагуров Т.А.

подпись

«31» мая 2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.03.02«Математические методы защиты информации»

Направление подготовки 01.03.02 Прикладная математика и информатика

Направленность (профиль) Программирование и информационные
технологии

Форма обучения очная

Квалификация бакалавр

Краснодар 2024

Рабочая программа дисциплины «Математические методы защиты информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.03.02 Прикладная математика и информатика.

Программу составил(и):

В.В. Подколзин, доцент, канд. физ.-мат. наук



Рабочая программа дисциплины «Математические методы защиты информации» утверждена на заседании кафедры информационных технологий протокол №20 от «21» мая 2024 г.

Заведующий кафедрой (разработчика)

В. В. Подколзин



подпись

Рабочая программа обсуждена на заседании кафедры информационных технологий протокол №20 от «21» мая 2024 г.

Заведующий кафедрой (выпускающей)

В. В. Подколзин



подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол №3 от «21» мая 2024 г.

Председатель УМК факультета

А. В. Коваленко



подпись

Рецензенты:

Бегларян М. Е., профессор кафедры социально-гуманитарных и естественнонаучных дисциплин СКФ ФГБОУВО «Российский государственный университет правосудия», канд. физ.-мат. наук, доцент

Рубцов Сергей Евгеньевич, кандидат физико-математических наук, доцент кафедры математического моделирования ФГБОУ «КубГУ»

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Курс посвящен изучению современных концепций информационной безопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах. Цель курса – научить студента методам информационной безопасности и их использованию в области защиты информации. Задачей курса является изложение теории информационной безопасности и практики применения алгоритмов криптозащиты.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению технологий, методов и средств производства и защиты программного обеспечения. Дать студентам математические основы защиты информации.

Отбор материала основывается на необходимости ознакомить студентов со следующей современной научной информацией:

- методы защиты информации;
- области применения защиты информации;
- о технологиях анализа шифров.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Студент в рамках курса должен знать области применения задач информационной безопасности; методы защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности. принципы построения и функционирования систем информационной безопасности; классификацию шифров; основы организации идентификации и цифровой подписи; принципы построения и применения паролей; уметь проводить анализ и определять оптимальный метод защиты информации; формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; формулировать и решать задачи организации процесса цифровой подписи; формулировать и решать задачи организации процесса идентификации; реализовать на языке программирования заданный метод защиты информации; решать задачи анализа шифра.

В качестве основной формы итогового контроля по рассматриваемой дисциплине предусмотрен экзамен.

1.2 Задачи дисциплины.

Основные задачи курса на основе системного подхода:

- Описать проблемную область информационной безопасности.
- Дать описание практического применения теории конечных полей в теории защиты информации.
- Расширить понятия о генерации псевдослучайных последовательностях.
- Расширить понятия о способах защиты информации.
- Расширить понятия о методах построения современных программных систем.
- Дать навыки практической работы с методами защиты информации.
- Дать навыки практической работы по решению задач идентификации.
- Дать навыки практической работы по решению задач цифровой подписи.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Математические методы защиты информации» относится к «Часть, формируемая участниками образовательных отношений» Блока 1 «Дисциплины (модули)» учебного плана.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

ПК-4 Способен активно участвовать в разработке системного и прикладного программного обеспечения

- Знать** ИПК-4.2 (06.001 D/03.06 Зн.2) Типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке системного и прикладного программного обеспечения
ИПК-4.3 (06.001 D/03.06 Зн.3) Методы и средства проектирования системного и прикладного программного обеспечения
ИПК-4.5 (06.015 В/16.5 Зн.3) Архитектура, устройство и функционирование вычислительных систем используемых в разработке системного и прикладного программного обеспечения
ИПК-4.7 (06.016 А/06.6 Зн.1) Возможности ИС, предметная область системное и прикладное программное обеспечение
ИПК-4.9 (06.016 А/30.6 Зн.2) Возможности ИС, методы разработки прикладного программного обеспечения
- Владеть** ИПК-4.17 (06.016 А/30.6 Тд.1) Качественный анализ рисков при разработке системного и прикладного программного обеспечения

ПК-5 Способен применять основные алгоритмические и программные решения в области информационно-коммуникационных технологий, а также участвовать в их разработке

- Знать** ИПК-5.1 (06.001 D/03.06 Зн.2) Типовые алгоритмические и программные решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения
ИПК-5.5 (06.015 В/16.5 Зн.1) Основы программные решения системного администрирования
ИПК-5.8 (06.015 В/16.5 Зн.4) Сетевые протоколы, программные решения их использования и реализации в области информационно-коммуникационных технологий
ИПК-5.9 (06.015 В/16.5 Зн.5) Основные алгоритмические и программные решения современных операционных систем
ИПК-5.11 (06.015 В/16.5 Зн.8) Современный отечественный и зарубежный опыт в области информационно-коммуникационных технологий
- Уметь** ИПК-5.12 (06.001 D/03.06 У.1) Использовать существующие алгоритмические и программные решения и шаблоны проектирования программного обеспечения
ИПК-5.13 (06.001 D/03.06 У.2) Применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов с использованием основных алгоритмических и программных решений в области информационно-коммуникационных технологий

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72часов), их распределение по видам работ представлено в таблице

Вид учебной работы	Всего часов	Семестры (часы)					
		7					
Контактная работа, в том числе:	40,2	40,2					
Аудиторные занятия (всего):	34	34					
Занятия лекционного типа							
Лабораторные занятия	34	34					
Занятия семинарского типа (семинары, практические занятия)							
Иная контактная работа:	6,2	6,2					
Контроль самостоятельной работы (КСР)	6	6					
Промежуточная аттестация (ИКР)	0,2	0,2					
Самостоятельная работа, в том числе:	31,8	31,8					
<i>Курсовая работа</i>							
<i>Проработка учебного (теоретического) материала</i>	14	14					
<i>Выполнение индивидуальных заданий (подготовка сообщений, презентаций)</i>	16	16					
<i>Реферат</i>							
Подготовка к текущему контролю	1,8	1,8					
Контроль:							
Подготовка к экзамену							
Общая трудоемкость	час.	72	72				
	в том числе контактная работа	40,2	40,2				
	зач. ед	2	2				

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы (темы) дисциплины, изучаемые в 7 семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1.	Базовые понятия и история развития информационной безопасности.	8			4	4
2.	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	10			6	4
3.	Шифры замены. Шифры перестановки. Шифры гаммирования.	8			4	4
4.	Блочные системы шифрования.	12			6	6
5.	Поточные системы шифрования.	14			8	6
6.	Идентификация. Цифровые подписи.	13,8			6	7,8

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
ИТОГО по разделам дисциплины		65,8			34	31,8
Контроль самостоятельной работы (КСР)		6				
Промежуточная аттестация (ИКР)		0,2				
Подготовка к текущему контролю						
Общая трудоемкость по дисциплине		72				

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

Не предусмотрено

Примечание: ЛР – отчет/защита лабораторной работы, КП – выполнение курсового проекта, КР – курсовой работы, РГЗ – расчетно-графического задания, Р – написание реферата, Э – эссе, К – коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.2 Занятия семинарского типа

Не предусмотрено

Примечание: ЛР – отчет/защита лабораторной работы, КП – выполнение курсового проекта, КР – курсовой работы, РГЗ – расчетно-графического задания, Р – написание реферата, Э – эссе, К – коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.3 Лабораторные занятия

№	Наименование лабораторных работ	Форма текущего контроля
1.	Основные шифры.	индивидуальное задание
2.	Стойкость шифров.	индивидуальное задание
3.	Конечные поля. Характеристика поля. Мультипликативная группа конечного поля.	индивидуальное задание
4.	Неприводимые многочлены. Порядок многочлена над конечным полем. Последовательности над конечным полем.	индивидуальное задание
5.	Последовательности над конечным полем. Псевдослучайные последовательности и их применение. Линейные рекуррентные последовательности над конечным полем. Линейные рекуррентные последовательности как псевдослучайные последовательности.	индивидуальное задание
6.	Математическая модель шифра замены. Поточные шифры простой замены. Блочные шифры простой замены.	индивидуальное задание
7.	Многоалфавитные шифры замены. Шифры перестановки. Маршрутные перестановки.	индивидуальное задание

№	Наименование лабораторных работ	Форма текущего контроля
8.	Табличное гаммирование.	индивидуальное задание
9.	Принципы построения блочных шифров.	индивидуальное задание
10.	Американский стандарт шифрования данных DES и его модификации.	индивидуальное задание
11.	Стандарт шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования	индивидуальное задание
12.	Поточные системы шифрования.	индивидуальное задание
13.	Линейные регистры сдвига.	индивидуальное задание
14.	Методы анализа поточных шифров.	индивидуальное задание
15.	Идентификация. Фиксированные пароли. Парольные фразы.	индивидуальное задание
16.	Цифровые подписи. Одноразовые цифровые подписи.	индивидуальное задание

Примечание: ЛР – отчет/защита лабораторной работы, КП - выполнение курсового проекта, КР - курсовой работы, РГЗ - расчетно-графического задания, Р - написание реферата, Э - эссе, К - коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.4 Примерная тематика курсовых работ (проектов) не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Изучение теоретического материала	Методические указания по организации самостоятельной работы студентов, утвержденные кафедрой информационных технологий, протокол №1 от 30.08.2019
2	Решение задач	Методические указания по организации самостоятельной работы студентов, утвержденные кафедрой информационных технологий, протокол №1 от 30.08.2019

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В соответствии с требованиями ФГОС в программа дисциплины предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; метод малых групп, разбор практических задач и кейсов.

При обучении используются следующие образовательные технологии:

– Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.

– Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал. Создание и использование диагностических тестов является неотъемлемой частью данной технологии.

– Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.

– Информационно-коммуникационные технологии (ИКТ) – расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы учащихся и повышению познавательной активности. В рамках ИКТ выделяются 2 вида технологий:

– Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения языку на всех уровнях.

– Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.

– Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.

– Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.

– Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.

– Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого учащегося.

– Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеназванных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные

процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Основные виды интерактивных образовательных технологий включают в себя:

– работа в малых группах (команде) - совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путём творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности;

– проектная технология - индивидуальная или коллективная деятельность по отбору, распределению и систематизации материала по определенной теме, в результате которой составляется проект;

– анализ конкретных ситуаций - анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений;

– развитие критического мышления – образовательная деятельность, направленная на развитие у студентов разумного, рефлексивного мышления, способного выдвинуть новые идеи и увидеть новые возможности.

Подход разбора конкретных задач и ситуаций широко используется как преподавателем, так и студентами во время лекций, лабораторных занятий и анализа результатов самостоятельной работы. Это обусловлено тем, что при исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и практических занятий.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные и методические материалы

4.1 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «название дисциплины».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме тестовых заданий, до **разноуровневых заданий** и **промежуточной аттестации** в форме вопросов и заданий к зачету.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Индивидуальные задачи (выполняются студентами самостоятельно и предоставляются в письменном виде).

1. Алгоритм DES. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
2. Алгоритм A5. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
3. Алгоритм Feal. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
4. Алгоритм Scurto1. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
5. Алгоритм IDEA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма Dragon. Реализовать в виде программного приложения с оконным интерфейсом.
6. Алгоритм ГОСТ 94. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
7. Алгоритм Mickey. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма Safer64. Реализовать в виде программного приложения с оконным интерфейсом.
8. Алгоритм Mosquito. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма RC5-64. Реализовать в виде программного приложения с оконным интерфейсом.

- Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
27. Алгоритм Blowfish. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
 28. Алгоритм Pike. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
 29. Алгоритм ГОСТ 2012. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
 30. Алгоритм DSA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы для промежуточной аттестации по итогам освоения дисциплины:

1. Группа. Подгруппа.
2. Группа постановок.
3. Кольцо. Идеалы. Классы вычетов.
4. Кольца полиномов.
5. Конечные поля.
6. Кольцо вычетов.
7. Алгоритмы умножения, обращения, вычисления НОД.
8. Извлечение корней в конечном поле.
9. Вычисление символа Якоби. Проверка на простоту.
10. Основные понятия и определения криптографической защиты информации.
11. Шифрование.
12. Аутентификация.
13. Система RSA. Детерминированные методы разложения.
14. Система RSA. Вероятностные методы разложения.
15. Дискретное логарифмирование в конечном поле. Задача Диффи-Хеллмана.
16. Шифрование с открытым ключом для группы вычислимого порядка.
17. Шифрование с открытым ключом для группы трудновычислимого порядка.
18. Цифровая подпись на группе трудновычислимого порядка.
19. Цифровая подпись на группе вычислимого порядка.
20. Схемы предъявления битов. Криптографические протоколы доказательства с нулевым разглашением.
21. Криптографические протоколы передачи информации со стиранием.
Криптографический протокол разделения секрета.
22. Криптографические протоколы управления ключами. Временная метка.
23. Основные понятия классической криптографии. Шифры замены и перестановки.
Блочные шифры.
24. Режимы шифрования.
25. Шифр DES.
26. Шифр FEAL.
27. Шифр IDEA.
28. Шифр ГОСТ 28147-89.
29. Шифр RC5.
30. Шифр Blowfish.
31. Шифр SAFER.
32. Шифр AES.

- 33. Шифр MD5.
- 34. Шифр ГОСТ Р 34.11-94.
- 35. Хэш-функция. Хэширование.

Критерий оценивания:

Оценка		
Удовлетворительно	Хорошо	Отлично
<ul style="list-style-type: none"> • если студент указал направление решения задачи и получил «удовлетворительно» по двум вопросам • если студент верно решил задачу; получил «хорошо» или «отлично» по ответу хотя бы на один вопрос 	<ul style="list-style-type: none"> • если студент в целом верно решил задачу и получил «хорошо» по двум вопросам • если студент в целом верно решил задачу и получил «удовлетворительно» по одному вопросу и «отлично» хотя бы на один вопрос 	<ul style="list-style-type: none"> • если студент верно решил задачу и получил «хорошо» хотя бы по одному вопросу и «отлично» по другому

Оценка «неудовлетворительно» выставляется при невозможности поставить оценку «Удовлетворительно», «Хорошо», «Отлично»

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

5.1 Основная литература:

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник /

- О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - <http://biblioclub.ru/index.php?page=book&id=438331>.
2. Лапони́на, О.Р. Криптографические основы безопасности / О.Р. Лапони́на. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016 – http://biblioclub.ru/index.php?page=book_red&id=429092&sr=1
 3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1
 4. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - https://biblioclub.ru/index.php?page=book_red&id=428998&sr=1

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1. Басалова, Г.В. Основы криптографии : курс лекций / Г.В. Басалова ; Национальный Открытый Университет "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2011. - 253 с. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=233689>
2. Сергеева, Ю.С. Защита информации. Конспект лекций [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : А-Приор, 2011. – https://biblioclub.ru/index.php?page=book_red&id=72670&sr=1
3. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – https://biblioclub.ru/index.php?page=book_red&id=480637&sr=1
4. Долозов, Н.Л. Программные средства защиты информации : конспект лекций / Н.Л. Долозов, Т.А. Гульятеева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=438307&sr=1
5. Бабенко, Л.И. Параллельные алгоритмы для решения задач защиты информации / Л.И. Бабенко, Е.А. Ищукова, И.Д. Сидоров. - Москва : Издательство Горячая линия-Телеком, 2014. - <https://e.lanbook.com/reader/book/63228/#1>.

5.3. Периодические издания:

1. Базы данных компании «Ист Вью» <http://dlib.eastview.com>
2. Электронная библиотека GREBENNIKON.RU <https://grebennikon.ru/>

5.4. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» <https://urait.ru/>
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» <http://www.biblioclub.ru/>
3. ЭБС «BOOK.ru» <https://www.book.ru>
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» <https://e.lanbook.com>

Профессиональные базы данных

1. Scopus <http://www.scopus.com/>
2. ScienceDirect <https://www.sciencedirect.com/>
3. Журналы издательства Wiley <https://onlinelibrary.wiley.com/>
4. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
5. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН <http://archive.neicon.ru>
6. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) <https://rusneb.ru/>
7. Президентская библиотека им. Б.Н. Ельцина <https://www.prlib.ru/>
8. База данных CSD Кембриджского центра кристаллографических данных (CCDC) <https://www.ccdc.cam.ac.uk/structures/>
9. Springer Journals: <https://link.springer.com/>
10. Springer Journals Archive: <https://link.springer.com/>
11. Nature Journals: <https://www.nature.com/>
12. Springer Nature Protocols and Methods: <https://experiments.springernature.com/sources/springer-protocols>
13. Springer Materials: <http://materials.springer.com/>
14. Nano Database: <https://nano.nature.com/>
15. Springer eBooks (i.e. 2020 eBook collections): <https://link.springer.com/>
16. "Лекториум ТВ" <http://www.lektorium.tv/>
17. Университетская информационная система РОССИЯ <http://uisrussia.msu.ru>

Информационные справочные системы

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа

1. КиберЛенинка <http://cyberleninka.ru/>;
2. Американская патентная база данных <http://www.uspto.gov/patft/>
3. Министерство науки и высшего образования Российской Федерации <https://www.minobrnauki.gov.ru/>;
4. Федеральный портал "Российское образование" <http://www.edu.ru/>;
5. Информационная система "Единое окно доступа к образовательным ресурсам" <http://window.edu.ru/>;
6. Единая коллекция цифровых образовательных ресурсов <http://school-collection.edu.ru/> .
7. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" <https://pushkininstitute.ru/>;
8. Справочно-информационный портал "Русский язык" <http://gramota.ru/>;
9. Служба тематических толковых словарей <http://www.glossary.ru/>;
10. Словари и энциклопедии <http://dic.academic.ru/>;
11. Образовательный портал "Учеба" <http://www.ucheba.com/>;
12. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--plai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ

1. Электронный каталог Научной библиотеки КубГУ
<http://megapro.kubsu.ru/MegaPro/Web>
2. Электронная библиотека трудов ученых КубГУ
<http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=6>
3. Среда модульного динамического обучения <http://moodle.kubsu.ru>
4. База учебных планов, учебно-методических комплексов, публикаций и конференций
<http://infoneeds.kubsu.ru/>
5. Библиотека информационных ресурсов кафедры информационных образовательных технологий <http://mschool.kubsu.ru;>
6. Электронный архив документов КубГУ <http://docspace.kubsu.ru/>
7. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ"
<http://icdau.kubsu.ru/>

6. Методические указания для обучающихся по освоению дисциплины (модуля)

По курсу предусмотрено проведение практических занятий, на которых дается прикладной систематизированный материал. В ходе занятий разбираются алгоритмы и структуры представления графов, а также приводятся примеры разработки программных приложений. После практического занятия рекомендуется выполнить упражнения, приводимые в аудитории для самостоятельной работы.

При самостоятельной работе студентов необходимо изучить литературу, приведенную в перечнях выше, для осмысления вводимых понятий, анализа предложенных подходов и методов разработки программ. Разрабатывая решение новой задачи студент должен уметь выбрать эффективные и надежные структуры данных для представления информации, подобрать соответствующие алгоритмы для их обработки, учесть специфику языка программирования, на котором будет выполнена реализация. Студент должен уметь выполнять тестирование и отладку алгоритмов решения задач с целью обнаружения и устранения в них ошибок.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

7.1 Перечень информационно-коммуникационных технологий

- Проверка домашних заданий и консультирование посредством электронной почты.
- Использование электронных презентаций при проведении практических занятий.

7.2 Перечень лицензионного и свободно распространяемого программного обеспечения

- Компилятор языка C++
- Программы для безопасной демонстрации и создания презентаций .
- Программы, поддерживающие OLE сервера.

8. Материально-техническое обеспечение по дисциплине (модулю)

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, проектором, программным обеспечением
2.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
3.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

Примечание: Конкретизация аудиторий и их оснащение определяется ОПОП.