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

УТВЕРЖДАЮ:
Проректор по учебной работе, качеству образования – первый проректор
_____ Т.А. Хагуров
подпись
«31» ____ 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД.В.03 ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Направление подготовки/специальность	02.03.01 Математика и компьютерные науки
Направленность (профиль) / специализация	Вычислительные, программные, информационные системы и компьютерные технологии; Математическое и компьютерное моделирование; Современная алгебра и криптография
Форма обучения	Очная
Квалификация	Бакалавр

Краснодар 2024

Рабочая программа дисциплины ФТД.В.03 Цифровая безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.01 Математика и компьютерные науки

Программу составил(и):

С.А. Шишкин, доц. кафедры вычислительной математики и информатики

подпись

Рабочая программа дисциплины ФТД.В.03 Цифровая безопасность утверждена на заседании кафедры вычислительной математики и информатики
протокол № 16 « 7 » мая 2024 г.
Заведующий кафедрой вычислительной математики и информатики

Гайденко С.В.
фамилия, инициалы

подпись

Утверждена на заседании учебно-методической комиссии факультета Математики и компьютерных наук
протокол № 3 « 14 » мая 2024 г.
Председатель УМК факультета Шмалько С.П.
фамилия, инициалы

подпись

Рецензенты:
Уртенов М.Х., д.-р. физ.-мат.н., профессор, заведующий кафедрой прикладной математики Кубанского государственного университета
Луценко Е.В., д.-р. э.н., канд. тех.н., профессор кафедры компьютерных технологий и систем Кубанского государственного аграрного университета

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины Курс посвящен изучению принципов административно-правовой защиты информации; освоению навыков применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; формированию навыков работы по обнаружению и защите от DDOS.

1.2 Задачи дисциплины

Освоить основные возможности инструментов и технологий для защиты данных. Сформировать практические навыки применения современных технологий для защиты данных и выявления нетипичного поведения сети.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «ФТД.В.03 Цифровая безопасность» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана. Дисциплина относится к факультативным дисциплинам, являющимся структурным элементом ОПОП ВО. В соответствии с рабочим учебным планом дисциплина изучается на 3 курсе по очной форме обучения. Вид промежуточной аттестации: зачет.

Дисциплине предшествуют дисциплины: Фундаментальная и компьютерная алгебра, Использование свободных и отечественных операционных систем, Основы компьютерных наук. Данная дисциплина является предшествующей в соответствии с учебным планом для дисциплины Информационная безопасность.

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:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ОПК-5 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ИОПК-5.1. Использует основные положения и концепции прикладного и системного программирования, архитектуры компьютеров и сетей (в том числе глобальных), современные языки программирования, технологии создания и эксплуатации программных продуктов и программных комплексов в профессиональной деятельности	**Знает** основные стандарты информационной безопасности **Умеет** применять методы анализа трафика и разрабатывать стратегии обеспечения устройств, приложений, сети **Владеет** навыками работы по обнаружению и защите от DDOS-атак
ИОПК-5.2. Применяет информационно-коммуникационные технологии в решении задач профессиональной деятельности, самостоятельно расширяет и углубляет знания в области информационных технологий	**Знает** основные правила защиты персональных данных и конфиденциальности в интернете **Умеет** Анализировать трафик и предотвращать сетевые вторжения **Владеет** навыками применения современных технологий создания брандмауэров и IDS-комплексов
ИОПК-5.3. Создает программные продукты и программные комплексы в области профессиональной деятельности с учетом основных требований информационной безопасности	**Знает** основные принципы административно-правовой защиты информации **Умеет** оперативно реагировать на различные угрозы информационной безопасности **Владеет** навыками применения, установки и настройки антивирусных систем и систем распознавания угроз и атак

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зачетные единицы (72 часа), их распределение по видам работ представлено в таблице

Виды работ		Всего часов	Форма обучения			
			очная		очно-заочная	заочная
			V семестр (часы)	X семестр (часы)	X семестр (часы)	X курс (часы)
Контактная работа, в том числе:		**38,2**	**38,2**			
Аудиторные занятия (всего):		**34**	**34**			
занятия лекционного типа		16	16			
лабораторные занятия		18	18			
практические занятия						
семинарские занятия						
Иная контактная работа:		**0,2**	**0,2**			
Контроль самостоятельной работы (КСР)		4	4			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**33,8**	**33,8**			
Реферат/эссе (подготовка)		10	10			
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным занятиям)		15,8	15,8			
Подготовка к текущему контролю		8	8			
Контроль:						
Подготовка к экзамену						
Общая трудоемкость	**час.**	**72**	**72**			
	в том числе контактная работа	**38,2**	**38,2**			
	зач. ед	**2**	**2**			

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 5 семестре (на 3 курсе) (очная форма обучения).

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Основные понятия цифровой безопасности	22	6		6	10
2.	Безопасность устройств и приложений	16	4		6	6
3.	Сетевая безопасность	12	4		2	6
4.	Антивирусное программное обеспечение	9,8	2		4	3,8
	ИТОГО по разделам дисциплины	59,8	16		18	25,8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	8				
	Общая трудоемкость по дисциплине	74				

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

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1.	Основные понятия цифровой безопасности	Основы цифровой безопасности: угрозы и риски	Опрос
2.	Основные понятия цифровой безопасности	Нормативно-правовые акты, связанные с защитой информации	Опрос
3.	Основные понятия цифровой безопасности	Защита персональных данных и конфиденциальности в интернете. Безопасность электронной почты и борьба с фишингом	Опрос
4.	Безопасность устройств и приложений	Безопасность объектов критической информационной инфраструктуры	Опрос
5.	Безопасность устройств и приложений	Безопасность мобильных устройств и приложений. Особенности обеспечения безопасности в финансовой сфере, онлайн-банкинг	Опрос
6.	Сетевая безопасность	Сетевая безопасность и защита от вредоносных программ. Анализ трафика и предотвращение вторжений	Опрос
7.	Сетевая безопасность	Основы кибербезопасности для бизнеса и организаций	Опрос
8.	Антивирусное программное обеспечение	Антивирусные программы и их роль в защите компьютера	Опрос

2.3.2 Занятия семинарского типа (практические / семинарские занятия/ лабораторные работы)

№	Наименование раздела (темы)	Тематика занятий/рабор	Форма текущего контроля
1.	Основные понятия цифровой безопасности	Анализ и сравнение различных методов аутентификации пользователей	ЛР
2.	Основные понятия цифровой безопасности	Правоприменительная практика в области информационной безопасности. Разбор практических ситуаций	Р
3.	Основные понятия цифровой безопасности	Изучение стандартов информационной безопасности и их применимость в различных отраслях	Опрос
4.	Безопасность устройств и приложений	Защита электронной почты, персональные данные в сети, угрозы в социальных сетях	Р
5.	Безопасность устройств и приложений	Объекты КИИ: типы и виды. Модель угроз	Р
6.	Безопасность устройств и приложений	Безопасность мобильных устройств. Анализ и сравнение различных протоколов безопасности для беспроводных сетей	ЛР
7.	Сетевая безопасность	Сетевая безопасность. Методы анализа трафика. Выявление нетипичного поведения в сети	ЛР
8.	Антивирусное программное обеспечение	Антивирусное программное обеспечение: типы и различия.	Опрос
9.	Антивирусное программное обеспечение	Разработка стратегии обеспечения устройств, приложений, сети	ЛР

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

При изучении дисциплины могут применятся электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.3 Примерная тематика курсовых работ (проектов)

Курсовые работы 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	Поиск и анализ литературы и электронных источников информации по заданной проблеме, изучение теоретического материала к лабораторным занятиям, подготовка к зачету	Например: Методические указания по организации самостоятельной работы по дисциплине «Анализ данных в профессиональной сфере», утвержденные вычислительной математики и информатики, протокол № 16 от 07.05.2024 г.

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, применяемые при освоении дисциплины (модуля)

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, практические занятия, проблемное обучение, модульная технология, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов проектных методик, мозгового штурма, разбора конкретных ситуаций, в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «ФТД.В.03 Цифровая безопасность».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме доклада-презентации по проблемным вопросам, практических заданий, и **промежуточной аттестации** в форме вопросов и заданий к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИОПК-5.1. Использует основные положения и концепции прикладного и системного программирования, архитектуры компьютеров и сетей (в том числе глобальных), современные языки программирования, технологии создания и эксплуатации программных продуктов и программных комплексов в профессиональной деятельности	**Знает** основные стандарты информационной безопасности **Умеет** применять методы анализа трафика и разрабатывать стратегии обеспечения устройств, приложений, сети **Владеет** навыками работы по обнаружению и защите от DDOS-атак	Вопрос для устного ответа 1-13 ЛР	Вопрос на зачете 1-15
2	ИОПК-5.2. Применяет информационно-коммуникационные технологии в решении задач профессиональной деятельности, самостоятельно расширяет и углубляет знания в области информационных технологий	**Знает** основные правила защиты персональных данных и конфиденциальности в интернете **Умеет** Анализировать трафик и предотвращать сетевые вторжения **Владеет** навыками применения современных технологий создания брандмауэров и IDS-комплексов	Вопрос для устного ответа 14-30 ЛР	Вопрос на зачете 16-38
3	ИОПК-5.3. Создает программные продукты и программные комплексы в области профессиональной деятельности с учетом основных требований информационной безопасности	**Знает** основные принципы административно-правовой защиты информации **Умеет** оперативно реагировать на различные угрозы информационной безопасности **Владеет** навыками применения, установки и настройки антивирусных систем и систем распознавания угроз и атак	Вопрос для устного ответа 31-41 ЛР	Вопрос на зачете 39-49

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов и заданий

Вопросы для устного опроса

1. Безопасность информации.
2. Источники и содержание угроз в информационной сфере.
3. Радиоэлектронная борьба.
4. Воздействие на сети.
5. Обеспечение информационной безопасности организации.

6. Характеристика эффективных стандартов по безопасности.
7. Планирование безопасной работы на персональном компьютере.
8. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
9. Административный уровень обеспечения информационной безопасности.
10. Категорирование объектов информатизации.
11. Общие положения по категорированию объектов информатизации.
12. Порядок проведения категорирования объектов на предприятий.
13. Классификация автоматизированных систем в составе объектов вычислительной техники.
14. Правовые основы сертификации и аттестации средств защиты информации.
15. Системная классификация средств защиты информации и их эффективности.
16. Шифрование с секретным ключом.
17. Объекты и элементы защиты в современных системах защиты информации.
18. Шифрование с открытым ключом.
19. Симметричные и несимметричные алгоритмы шифрования.
20. Модели защиты информации.
21. Компьютерные вирусы.
22. Формы атак на информацию.
23. Общие принципы построения защищенных ОС.
24. Методы защиты компьютерной информации.
25. Управление безопасностью в защищенных ОС.
26. Функции, задачи защиты информации.
27. Аутентификация субъектов и объектов защиты информаии.
28. Определение потенциально возможных нарушителей защиты компьютерной информации.
29. Структура и содержание общей модели оценки уязвимости.
30. Задача защиты и информации в корпоративных сетях.
31. Брандмауэры и их характеристики.
32. Физические средства защиты информации.
33. Управление доступом к данным.
34. Криптографические средства защиты информации.
35. Защита электронной почты.
36. Защита IP сетей.
37. Оперативно-диспетчерское управление защитой информации.
38. Защита средств сетевого управления.
39. Планирование защиты информации.
40. Обеспечение повседневной деятельности и службы защиты информации.
41. Роль стандартов информационной безопасности и их анализ.

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

1. Понятие безопасности и её составляющие. Безопасность информации.
2. Обеспечение информационной безопасности: содержание и структура понятия.
3. Источники и содержание угроз в информационной сфере.
4. Радиоэлектронная борьба. Воздействие на сети.
5. Основные положения государственной информационной политики Российской Федерации.
6. Виды защищаемой информации в сфере государственного и муниципального

7. управления.
8. Обеспечение информационной безопасности организации.
9. Характеристика эффективных стандартов по безопасности.
10. Планирование безопасной работы на персональном компьютере.
11. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.
12. Административный уровень обеспечения информационной безопасности.
13. Категорирование объектов информатизации.
14. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.
15. Классификация автоматизированных систем в составе объектов вычислительной техники.
16. Правовые основы сертификации и аттестации средств защиты информации.
17. Радиоэлектронная борьба. Воздействие на сети.
18. Системная классификация средств защиты информации и их эффективности.
19. Шифрование с секретным ключом.
20. Объекты и элементы защиты в современных системах защиты информации.
21. Шифрование с открытым ключом.
22. Симметричные и несимметричные алгоритмы шифрования.
23. Модели защиты информации.
24. Компьютерные вирусы.
25. Формы атак на информацию.
26. Общие принципы построения защищенных ОС.
27. Методы защиты компьютерной информации.
28. Управление безопасностью в защищенных ОС.
29. Функции, задачи защиты информации.
30. Аутентификация субъектов и объектов защиты информаии.
31. Определение потенциально возможных нарушителей защиты компьютерной
32. информации.
33. Проектирование систем защиты информации
34. Алгоритмы аутентификации.
35. Структура и содержание общей модели оценки уязвимости.
36. Задача защиты и информации в корпоративных сетях.
37. Аппаратные и программные средства информации.
38. Брандмауэры и их характеристики.
39. Физические средства защиты информации.
40. Управление доступом к данным.
41. Криптографические средства защиты информации.
42. Защита электронной почты.
43. Защита IP сетей.
44. Оперативно-диспетчерское управление защитой информации.
45. Защита средств сетевого управления.
46. Планирование защиты информации.
47. Обеспечение повседневной деятельности и службы защиты информации.
48. Роль стандартов информационной безопасности и их анализ.
49. Анализ некоторых алгоритмов электронной подписи.

Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по каждому алгоритму из всех разделов, знает постановки задач анализа данных, программно реализует алгоритмы обработки данных, знает все особенности методов, владеет трансформированием архитектуры и структуры систем сбора, хранения, обработки больших данных.

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести постановки математических задач и алгоритмов их решения, не знает проблемные ситуации в обсуждаемых задачах.

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.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Учебная литература

1) Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://www.biblioonline.ru/bcode/434171 (дата обращения 30.08.2019)

2) Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю.Н. Загинайлов. – М. ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения 30.08.2019)

3) Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : 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. – 113 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения 30.08.2019)

4) Основы информационной безопасности [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/10/10/info

5) Антивирусная защита компьютерных систем [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/2259/155/info

6) Безопасность сетей [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/102/102/info

7) Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

8) Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А. В.Артемов. — Электрон. текстовые данные. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — 2227-8397. — Режим доступа:http://www.iprbookshop.ru/33430.html

9) Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Электрон. Текстовые данные. — М. : Евразийский открытый институт, 2012. — 311 с. — 978-5-374-00301-7. — Режим доступа: http://www.iprbookshop.ru/10677.html

10) Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва :Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021.— 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/101992.html

5.3. 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» 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. Научная электронная библиотека (НЭБ) http://www.elibrary.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. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;

3. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .

4. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru

2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/

3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;

4. Электронный архив документов КубГУ http://docspace.kubsu.ru/

5. 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)

Для сдачи зачета надо изучить теоретический материал таблицы п.2.3.1. Также студент должен научиться выполнять практические задания по темам этих разделов на лабораторных занятиях. Самостоятельная работа студента включает в себя подготовку к лабораторным занятиям и зачету. Эти виды самостоятельной работы студентов контролируется в ходе проверки домашних заданий и зачета. Теоретические вопросы к зачету приведены в пункте 4. Зачет выставляется после успешного выполнения лабораторных работ.

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.

6. Материально-техническое обеспечение по дисциплине (модулю)

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Visual Studio Code (Python) MS Office PyCharm kaspersky security center
Учебные аудитории для проведения лабораторных работ. специальное помещение, оснащенное компьютерной техникой	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: компьютерная техника по численности студентов (системный блок, монитор, клавиатура, мышь)	Visual Studio Code (Python) MS Office PyCharm kaspersky security center

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с

возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Visual Studio Code (Python) MS Office PyCharm kaspersky security center
Помещение для самостоятельной работы обучающихся (специальное помещение, оснащенное компьютерной техникой)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Visual Studio Code (Python) MS Office PyCharm kaspersky security center