Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кубанский государственный университет»

Факультет компьютерных технологий и прикладной математики
Кафедра вычислительных технологий

УТВЕРЖДАЮ
Проректор по учебной работе, качеству образования – первый проректор
_____Хагуров Т.А.
подпись

«_30_» _____мая_____2025

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.25 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки/специальность_02.03.02 **Фундаментальная информатика и информационные технологии**
(код и наименование направления подготовки/специальности)

Направленность (профиль) /специализация
Математическое и программное обеспечение компьютерных технологий

Программа подготовки *академический бакалавриат*

Форма обучения *очная*

Квалификация выпускника *бакалавр*

Краснодар 2025

Рабочая программа дисциплины «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Программу составили:

Шиян Валерий Игоревич, ст. преподаватель
Ф.И.О., должность, ученая степень, ученое звание — подпись

Приходько Татьяна Александровна, доцент, к. т. н.
Ф.И.О., должность, ученая степень, ученое звание — подпись

Рабочая программа дисциплины утверждена на заседании кафедры вычислительных технологий протокол № 7 «07» мая 2025 г.

И.о. заведующего кафедрой (разработчика) Еремин А.А.
фамилия, инициалы — подпись

Рабочая программа дисциплины обсуждена на заседании кафедры вычислительных технологий протокол № 7 «07» мая 2025 г.

И.о. заведующего кафедрой (разработчика) Еремин А.А.
фамилия, инициалы — подпись

Утверждена на заседании учебно-методической комиссии факультета Компьютерных Технологий и Прикладной Математики протокол № 4 от «23» мая 2025 г

Председатель УМК факультета Коваленко А.В.
фамилия, инициалы — подпись

Рецензенты:

Гаркуша О.В., доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», кандидат физико-математических наук.

Схаляхо Ч.А., доцент КВВУ им. С.М. Штеменко, к.ф.-м.н., доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель и задачи освоения дисциплины

Целью преподавания и изучения дисциплины «Информационная безопасность» является формирование у студентов способности оценивать угрозы информационной безопасности и разрабатывать архитектурные и функциональные спецификации создаваемых систем и средств по ее защите, а также разрабатывать методы реализации и тестирования таких систем.

1.2 Задачи дисциплины

Студент должен знать основные понятия, методы, алгоритмы и технологии защиты информации; уметь применять теории и методы по обеспечению информационной безопасности; владеть технологиями реализации систем такой защиты.

1.3 Место дисциплины (модуля) в образовательной программе

Дисциплина «Информационная безопасность» относится к вариативной части блока Б1 Дисциплины (модули).

Для изучения дисциплины необходимо знание дисциплин “Дискретная математика”, “Алгебра”, “Основы программирования”, “Теория алгоритмов и вычислительных процессов”, “Операционные системы”, “Компьютерные сети”. Знания, получаемые при изучении основ защиты информации, используются при изучении таких дисциплин профессионального цикла учебного плана бакалавра как “Программирование в компьютерных сетях”, “Криптографические протоколы”, а также при работе над выпускной работой.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих **профессиональных компетенций и соотнесенных с ними индикаторов достижения компетенций:** ОПК-5; ПК-1.

Код и наименование индикатора*	**Результаты обучения по дисциплине** ***(знает, умеет, владеет (навыки и/или опыт деятельности))***
ОПК-5 Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	
ОПК-5.1. Знает методику установки и администрирования информационных систем и баз данных. Знаком с содержанием Единого реестра российских программ.	Знает содержание информационной безопасности и ее место в системе национальной безопасности, основные угрозы и методы защиты от них, системные методологии, международные и профессиональные стандарты в области информационной безопасности.
ОПК-5.2. Умеет реализовывать техническое сопровождение информационных систем и баз	Умеет использовать углубленные теоретические и практические знания в области информационной

Код и наименование индикатора*	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
данных.	безопасности.
ОПК-5.3. Имеет практические навыки установки и инсталляции программных комплексов, применения основ сетевых технологий.	Владеет навыками использования технологий обеспечивающих создание безопасных программных решений.
ПК-1 Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии	
ПК-1.1. Знает основы научно- исследовательской деятельности в области информационных технологий, имеет научные знания в теории информационных систем.	Знает содержание информационной безопасности и ее место в системе национальной безопасности, основные угрозы и методы защиты от них, системные методологии, международные и профессиональные стандарты в области информационной безопасности.
ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности.	Умеет использовать углубленные теоретические и практические знания в области информационной безопасности.
ПК-1.3. Имеет практический опыт научно-исследовательской деятельности в области информационных технологий.	Владеет навыками использования технологий обеспечивающих создание безопасных программных решений.

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

№ п.п.	Индекс компе-тенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающие должны		
			знать	уметь	владеть
1	ОПК-5	способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	содержание информационной безопасности и ее место в системе национальной безопасности, основные угрозы и методы защиты от них, системные методологии, международные и профессиональные стандарты в области информационной безопасности	использовать углубленные теоретические и практические знания в области информационной безопасности	навыками использования технологий обеспечиваю щих создание безопасных программных решений
2	ПК-1	способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания,	содержание информационной безопасности и ее место в системе национальной безопасности, основные угрозы и методы защиты от них, системные методологии,	использовать углубленные теоретические и практические знания в области информационно й безопасности	навыками использования технологий обеспечивающих создание безопасных программных решений

		современные языки программирования и программное обеспечение; операционные системы и сетевые технологии	международные и профессиональные стандарты в области информационной безопасности		

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 4 зач. ед. (144 часа), их распределение по видам работ представлено в таблице (для студентов ОФО).

Вид учебной работы	Всего часов	Семестры (часы)	
		7	
Контактная работа в том числе:	**72.3**	**72.3**	
Аудиторные занятия (всего):	68	68	
В том числе:			
Занятия лекционного типа	34	34	
Занятия семинарского типа (семинары, практ. занятия)			
Лабораторные занятия	34	34	
Иная контактная работа	0.3	0.3	
Контроль самостоятельной работы (КСР)	4	4	
Промежуточная аттестация (ИКР)			
Самостоятельная работа, в том числе	**36**	**36**	
В том числе:			
Курсовая работа			
Проработка учебного (теоретического) материала	15	15	
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	15	15	
Реферат			
Подготовка к текущему контролю	6	6	
Контроль: экзамен	**35.7**	**35.7**	
Общая трудоёмкость	**в час**	**144**	
	в т.ч. контактная работа	**72.3**	

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины. Разделы дисциплины, изучаемые в 7 семестре *(очная форма)*

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Содержание понятия безопасность и его структура. Проектирование алгоритмов поддержки информационной безопасности.	16	6		6	4

2.	Стандарты информационной безопасности.	20	8		8	4
3.	Сценарий Идентификация-Аутентификация- Авторизация и варианты реализации.	20	6		6	8
4.	Модели управления доступом к информации. Модели поддержания целостности информации	24	8		8	8
5.	Аудит вычислительной системы и архивация. Анализ уязвимости системы. DLP-системы. Системы обнаружения вторжений	23.7	6		6	11.7
	ИТОГО по разделам дисциплины	103.7	34		34	35.7
	Контроль самостоятельной работы (КСР)	0,3				
	Общая трудоёмкость по дисциплине	144				

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Содержание понятия безопасность и его структура	Виды безопасности и связи между ними. Анализ угроз информационной безопасности. Правовая поддержка организации информационной безопасности. Смысл компьютерной безопасности, ее основные требования. Основные понятия актуализации компьютерной безопасности.	ЛР
2	Проектирование алгоритмов поддержки информационной безопасности	Организация вычислений на графе. Кодирующие и декодирующие преобразования. Алгоритмы защиты данных, основанные на комбинаторике и теории чисел.	ЛР
3	Стандарты информационной безопасности	Критерии безопасности компьютерных систем (Оранжевая книга). ISO/IEC 17799:2002 “Управление информационной безопасностью”. ISO 15408 “Общие критерии безопасности информационных технологий” “CommonCriteria” (ОК). Российские стандарты в области информационной безопасности.	ЛР
4	Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации	Подходы к идентификации и аутентификации. Понятие полномочий и ролей, их виды. Реализация сценария идентификации- аутентификации-авторизации в операционных системах Windows и Unix.	ЛР

5	Модели управления доступом к информации	Монитор безопасности. Основные политики доступа. Модель HRU. Модель Белла-ЛаПадулы. Модель МакЛина. Модель Take-Grant. Модель Китайская стена.	ЛР
6	Модели поддержания целостности информации	Ролевые модели доступа. Модель Биба. Модель Кларка-Вильсона.	ЛР
7	Аудит вычислительной системы и архивация	Смысл аудита и ресурсы, необходимые для его осуществления. Способы и инструментарий для аудита в операционных системах Windows и Unix. Выполнение backup-а системы, архивация данных.	ЛР
8	Анализ уязвимости системы. DLP-системы	Классификация уязвимостей. Пример уязвимости и ее использование. Методология гипотетического дефекта. Обзор DLP-систем	ЛР
9	Системы обнаружения вторжений	Обзор моделей обнаружения вторжений. Архитектура IDS-системы. Средства детекции вторжений в операционных системах.	ЛР
10	Поддержка информационной безопасности в вычислительных сетях	Анализ стека протоколов ISOOSI с точки зрения информационной безопасности. Межсетевой экран. Технология сетей VPN. Протоколы защиты информации различных уровней. Протокол Kerberos. Инфраструктура управления открытыми ключами.	ЛР

2.3.2 Занятия семинарского типа

Учебным планом не предусмотрены.

2.3.3 Лабораторные занятия

№ работы	№ раздела дисциплины	Наименование лабораторных работ
1–5	1	Проектирование алгоритмов поддержки информационной безопасности.
6	2	Стандарты информационной безопасности.
7	2	Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации.
8-9	3	Модели управления доступом к информации.
10	3	Модели поддержания целостности к информации
11	4	Аудит вычислительной системы и архивация.
12	4	Анализ уязвимости системы. DLP-системы
13	5	Системы обнаружения вторжений
14-15	5	Поддержка информационной безопасности в вычислительных сетях
16	5	Зловредное программное обеспечение

2.3.4 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

2.3.5 Самостоятельное изучение разделов дисциплины

Раздел 1. Законодательные акты: О безопасности, Доктрина информационной безопасности РФ, Об охране интеллектуальной собственности, О персональных данных, Об информации, информационных технологиях и о защите информации, О государственной тайне, О международном обмене информацией.

Раздел 2. Учебники и пособия по проектированию структур данных и алгоритмов их обработки. Руководства, учебники и пособия по языку Visual C++ и работе в среде Visual Studio 2012 и выше.

Раздел 3. Международные и российские стандарты РФ по информационной безопасности: закон РФ "О техническом регулировании", "Критерии оценки доверенных компьютерных систем" (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC − Оранжевая книга), ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" (Evaluation Criteria for IT security − ОК),ГОСТ Р 50739, ГОСТ Р 50922-96, ГОСТ Р 51188-98, ГОСТ Р 50739-95.

Раздел 4. Руководства и учебники по администрированию в операционных системах Windows, Unix, Linux.

Раздел 5. Учебники и пособия из рекомендованного списка литературы. Руководства и учебники по администрированию в операционных системах Windows, Unix, Linux, учебные ресурсы в internet, а также обучающие материалы от производителей антивирусного ПО.

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
7	Л	Компьютерные презентации и обсуждение	34
	ЛР	Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии, сведений из области информационной безопасности, программирование алгоритмов	34
Итого:			68

4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1 Фонд оценочных средств для проведения текущего контроля

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ОПК-5.1. Знает методику установки и	Знает классификацию информационных угроз,	Опрос по теме	Вопросы 1-13, выносимые на

	администрирования информационных систем и баз данных. Знаком с содержанием Единого реестра российских программ.	основные качества защищенной информации в ИС, понимает смысл политики безопасности. Знаком с понятиями несанкционированного доступа, уязвимости, атаки и их видов.	лабораторных работ.	зачет
2	ОПК-5.2. Умеет реализовывать техническое сопровождение информационных систем и баз данных.	Умеет применять модели доступа к данным, понимает назначение и структуру стандартов информационной безопасности. Знает о различных видах атак, таких как сниффинг, спуффинг, hijacking, DOS-атака, DDOS-атака и SYN-атака.	Опрос по теме лабораторных работ.	Вопросы 1-13, выносимые на зачет
3	ОПК-5.3. Имеет практические навыки установки и инсталляции программных комплексов, применения основ сетевых технологий.	Имеет практические навыки определения алгоритмической разрешимости безопасности системы в модели HRU. Знает о видах данных, которые должны находиться в открытом доступе, и уровнях секретности данных, регламентируемых законом РФ "О государственной тайне".	Опрос по теме лабораторных работ.	Вопросы 1-13, выносимые на зачет
4	ПК-1.1. Знает основы научно-исследовательской деятельности в области информационных технологий, имеет научные знания в теории информационных систем.	Знает классификацию информационных угроз, основные качества защищенной информации в ИС, смысл политики безопасности, виды несанкционированного доступа, понятия уязвимости, атаки и ее структуры. Также студент должен знать виды моделей доступа к данным и назначение стандартов информационной безопасности.	Опрос по теме лабораторных работ.	Вопросы 1-28, выносимые на экзамен
5	ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности.	Умеет применять полученные знания для решения задач, связанных с обеспечением информационной безопасности, таких как идентификация, аутентификация и авторизация пользователей, анализ различных моделей полномочий (HRU, Белла-ЛаПадулы, Мак-Лина), классификация зловредного ПО и методов социальной инженерии.	Опрос по теме лабораторных работ.	Вопросы 1-28, выносимые на экзамен
6	ПК-1.3. Имеет практический опыт научно-исследовательской деятельности в области информационных технологий.	Имеет практический опыт применения средств информационной безопасности, таких как VPN, сетевые экраны, системы аудита в ОС Windows. Также студент должен уметь анализировать структуру угроз информационной безопасности и применять основные понятия ИБ на практике.	Опрос по теме лабораторных работ.	Вопросы 1-28, выносимые на экзамен

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств для итоговой аттестации (зачет и экзамен в 7 семестре).

Оценка успеваемости осуществляется по результатам:
- выполнения лабораторных работ;
- ответа на экзамене

Текущий контроль включает контрольную работу по итогам первой половины курса.

4.2.1 Перечень вопросов к зачету

1. Классификация информационных угроз.
2. Основные качества защищенной информации в ИС.
3. В чем смысл политики безопасности.
4. Что такое несанкционированный доступ (НСД) и их виды.
5. Что такое уязвимость, атака, структура атаки и возможные виды атак.
6. Виды моделей доступа к данным, их характеристика.
7. Назначение стандартов информационной безопасности. Структура стандартов.
8. Что такое сниффинг, спуффинги hijacking.
9. Что такое DOS-атака, DDOS-атака ,SYN-атака.
10. Является ли алгоритмически разрешимым свойство быть безопасной системой в модели HRU.
11. Какого вида данные обязаны находиться в открытом доступе.
12. Назовите уровни секретности данных, которые регламентирует закон РФ “О государственной тайне”.

4.2.2 Перечень вопросов к экзамену

1. Классификация информационных угроз.
2. Основные качества защищенной информации в ИС.
3. В чем смысл политики безопасности.
4. Что такое несанкционированный доступ (НСД) и их виды.
5. Что такое уязвимость, атака, структура атаки и возможные виды атак.
6. Виды моделей доступа к данным, их характеристика.
7. Назначение стандартов информационной безопасности. Структура стандартов.
8. Что такое сниффинг, спуффинги hijacking.
9. Что такое DOS-атака, DDOS-атака ,SYN-атака.
10. Является ли алгоритмически разрешимым свойство быть безопасной системой в модели HRU.
11. Какого вида данные обязаны находиться в открытом доступе.
    Назовите уровни секретности данных, которые регламентирует закон РФ“О государственной тайне”.
12. Механизм идентификации, аутентификации и авторизации в ОС Unix.
13. Механизм идентификации, аутентификации и авторизации в ОС Windows.
14. Биометрические методы аутентификации
15. Механизм одноразовых паролей
16. Протокол аутентификации Kerberos
17. Основные положения дискреционной модели полномочий HRU
18. Основные положения мандатной модели полномочий Белла-ЛаПадулы

19. Модель полномочий Мак-Лина.
20. Классификация зловредного программного обеспечения.
21. Особенности полиморфного вируса и руткита.
22. Основные положения VPN-сети.
23. Назначение методов социальной инженерии и их формы.
24. Назначение и формы аудита в ОС Windows.
25. Назначение и механизм сетевого экрана.
26. Характеристика средств информационной безопасности в рамках стека протоколов ISO OSI.
27. Структура угроз информационной безопасности.
28. Содержание основных понятий ИБ: «защищенность данных», «уязвимость», «атака», «злоумышленник» и др. Их отражение в стандартах ИБ.

4.2.3 Образцы билетов

Билет №1

1. Правила NRU и NWD . Области использования этих правил.
2. Характеристика схемы симметричного шифрования. Достоинства и недостатки этой схемы.
3. Сколько времени необходимо на расшифровку ключа алгоритма DES на компьютере с быстродействием 1000 млрд. операций в секунду если один ключ расшифровывается за 10 операций.

Билет №2

1. Основные компоненты модели Take-Grant. Понятие графа доступов и его пример.
2. Протокол аутентификации Kerberos.
3. Постройте матрицу управления доступом для медицинского учреждения, в котором врачи могут читать писать истории болезней и предписания по лечению, а медицинские сестры могут читать и писать предписания по лечению, но ничего не должны знать об истории болезней.

4.2.4 Критерии оценивания к экзамену

Оценка «отлично»: точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «хорошо»: при ответе на один вопрос даны точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями; при ответе на второй вопрос имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или

неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «удовлетворительно»: при ответе на оба вопроса имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «неудовлетворительно»: отсутствует ответ хотя бы на один из вопросов или имеются существенные неточности в формулировках алгоритмов, теорем, приведены неправильные доказательства; неверные определения математических объектов и неправильные определения объектов, характеризующихся неформализованными понятиями.

5. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Основная литература

1. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем[Электронный ресурс]: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - Москва: ИНФРА-М, 2021. -118 с. + Доп. материалы. - (Высшее образование: Бакалавриат).- Режим доступа: https://znanium.com/read?id=362430.
2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2022. - 592 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Режим доступа: https://znanium.com/read?id=389857.

5.2 Дополнительная литература

3. М. Ховард, Д. Лебланк Защищенный код. □ М.: ИД Русская редакция, 2004.− 704 с.
4. Проскурин В. Г. Защита программ и данных. □ М.: ИДАкадемия, 2012.− 208 с.
5. Т. Howlett Open source security tools. Practical applications for security. □Prantice Hall, 2004.− 600 p.
6. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие.− М.: ИД Форум – Инфра, 2013.− 416 с.
7. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. □ М.: Горячая линия – Телеком, 2000.− 452 с.
8. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. □ М.: Академия, 2008.− 256 с.
9. Девянин П. Н. Модели безопасности компьютерных систем. Учебное пособие.−М.: Академия, 2005.− 144 с

5.2 Периодическая литература

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

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. Scopus http://www.scopus.com/
2. Science Direct 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. Nature Journals https://www.nature.com/siteindex/index.html
11. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
12. Springer Materials http://materials.springer.com/
13. Springer Journals Archive: https://link.springer.com/
14. Nano Database https://nano.nature.com/
15. Springer eBooks: 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--p1ai/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 учёных 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://mschool.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)

Для освоения учебного материала студенту необходимо ознакомиться со структурой курса и методикой овладения материалом. Весь курс построен от простого к сложному, и каждая его тема основана на материалах предыдущих тем. В этой связи студенту необходимо не терять логику курса и строго ей следовать. В лекционном материале даются, как правило, теоретические сведения, которые раскрываются на практических примерах. Для закрепления теоретических знаний студент получает индивидуальное задание к циклу лабораторных работ, который охватывает весь теоретический материал. Каждая лабораторная работы защищается по мере выполнения. Таким образом, выполняя весь цикл лабораторных работ, студент получает и осваивает знания в соответствии с компетенциями курса. По выступлениям на круглом столе с преподавателем согласовывается тема выступления и готовится само выступление. Во время текущей аттестации могут проводиться контрольные опросы по начитанному теоретическому и практическому материалу.

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 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Наименование специальных помещений	Оснащённость специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа (ауд. 129, 131, А305).	Мебель: учебная мебель Технические средства обучения: проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО)	PowerPoint, доступ к Microsoft Teams
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации ауд. 129, 131, А305	Мебель: учебная мебель Технические средства обучения: экран, компьютер Оборудование: кондиционер	PowerPoint, доступ к Microsoft Teams

Учебные аудитории для проведения лабораторных работ. Лаборатория (ауд. 102-106, А301-303).	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	системы программирования на языках высокого уровня, сетевой доступ к ресурсам, в частности C++, Object Pascal и пр. с возможностью многопользовательской работы

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащённые компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащённость 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)	Доступ печатным и электронным информационным ресурсам
Помещение для самостоятельной работы обучающихся (ауд. 146)	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)	1. Microsoft Visual Studio 2012+ : Visual C++, C# 2. OracleVirtualBoxv 5.1 + 3. Python