



1920

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего
образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)**

Филиал в г. Славянске-на-Кубани

Факультет математики, информатики, биологии и технологии

**Кафедра математики, информатики, естественнонаучных и
общетехнических дисциплин**



УТВЕРЖДАЮ:

Проректор по учебной работе,
качеству образования - первый
проректор

Т.А. Хагуров

«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.19.02 ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Направление подготовки 44.03.01 Педагогическое образование

Направленность (профиль) Информатика

Форма обучения очно-заочная

Квалификация бакалавр

Краснодар 2025

Рабочая программа производственной практики «Основы кибербезопасности» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 44.03.01 Педагогическое образование утвержденному приказом Министерства образования и науки Российской Федерации от 22 февраля 2018 г. № 121, зарегистрировано в Минюсте России 15.03.2018 № 50362.

Программу составил:

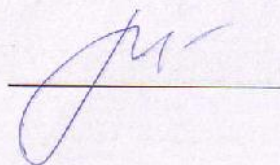
Письменный Р.Г.

доцент кафедры математики, информатики,
естественнонаучных и общетехнических дисциплин,
кандидат физико-математических наук



Рабочая программа производственной практики «Основы кибербезопасности» утверждена на заседании кафедры математики, информатики, естественнонаучных и общетехнических дисциплин
протокол № 9 от 06.05.2025 г.

Зав. кафедрой математики, информатики,
естественнонаучных и общетехнических
дисциплин Радченко С. А.,

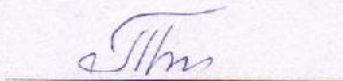


Утверждена на заседании учебно-методической комиссии филиала,
протокол № 9 от 14.05.2025 г.

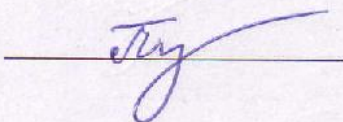
Председатель УМК филиала Поздняков С. А.



Рецензенты:



Пышная Л.Н., директор МАОУ СОШ № 18 имени Героя Советского Союза И. К.. Боронина, г. Славянска-на-Кубани
МО Славянский район



Пушечкин Н.П., доцент, канд. физ.-мат. наук, доцент кафедры
МИЕиОД, филиала КубГУ в г.Славянске-на-Кубани

Содержание

Содержание.....	3
1 Цели и задачи изучения дисциплины.....	4
1.1 Цель освоения дисциплины.....	4
1.2 Задачи дисциплины.....	4
1.3 Место дисциплины в структуре образовательной программы.....	4
1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.....	4
2 Структура и содержание дисциплины	6
2.1 Распределение трудоёмкости дисциплины по видам работ	6
2.2 Структура дисциплины.....	6
2.3 Содержание разделов дисциплины	7
2.3.1 Занятия лекционного типа.....	7
2.3.2 Занятия семинарского типа	7
2.3.3 Лабораторные занятия	8
2.3.4 Примерная тематика курсовых работ.....	8
2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	8
3 Образовательные технологии, применяемые при освоении дисциплины.....	9
3.1 Образовательные технологии при проведении лекций	9
3.3 Образовательные технологии при проведении лабораторных занятий.....	10
4 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации....	11
4.1 Структура оценочных средств для текущей и промежуточной аттестации.....	11
4.2 Показатели, критерии и шкала оценки сформированных компетенций	11
4.3 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.....	12
4.1.4 Зачетно-экзаменационные материалы для промежуточной аттестации	16
5 Перечень учебной литературы, информационных ресурсов и технологий	17
5.1 Учебная литература.....	17
5.2 Периодические издания.....	17
5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы	18
6 Методические указания для студентов по освоению дисциплины.....	20
6.1 Общие рекомендации по самостоятельной работе обучающихся	20
6.2 Рейтинговая система оценки текущей успеваемости студентов	21
6.3 Организация процедуры промежуточной аттестации	21
7 Материально-техническое обеспечение по дисциплине.....	22

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Целью освоения дисциплины «Основы кибербезопасности» является:

- формирование у обучающихся системных знаний и практических навыков в области защиты информации;
- развитие абстрактного мышления, вычислительной, алгоритмической культур и общей математической и информационной культуры.

1.2 Задачи дисциплины

Изучение дисциплины «Основы кибербезопасности» направлена на формирование у студентов компетенции:

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

ОПК-7 Способен взаимодействовать с участниками образовательных отношений в рамках реализации образовательных программ

ПК-2 Способен применять знания математики и информатики при реализации образовательного процесса.

ПК-3 Способен организовывать деятельность обучающихся, направленную на развитие интереса к математике и информатике в рамках урочной и внеурочной деятельности.

В соответствии с этим ставятся следующие задачи дисциплины:

- Изучить ключевые концепции кибербезопасности (угрозы, атаки, методы защиты) для их последующего изложения в учебном процессе.
- Освоить нормативную базу (GDPR, 152-ФЗ, ФСТЭК) и методики её преподавания.
- Проанализировать современные образовательные стандарты и программы в области ИБ.
- Научиться демонстрировать примеры кибератак (фишинг, SQL-инъекции) с использованием симуляторов (Kali Linux, CyberRange).
- Отработать методы объяснения сложных тем (криптография, сетевые атаки) через интерактивные форматы (кейсы, геймификацию).
- Разрабатывать лабораторные работы по настройке средств защиты (фаерволы, VPN, антивирусы).

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Основы кибербезопасности» относится к обязательной части учебного плана. Она изучается в 3семестре. Для ее освоения студенты используют знания, умения, навыки, сформированные в ходе изучения школьного курса информатики.

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

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

Код и наименование индикатора*	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
ИУК-1.1. Осуществляет поиск необходимой информации, опираясь на результаты анализа поставленной задачи	знает методы критического анализа и оценки современных научных достижений, основные принципы критического анализа
	умеет собирать данные по сложным научным проблемам, относящимся к профессиональной области

Код и наименование индикатора*	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
	владеет навыками исследования профессиональных проблем с применением анализа, синтеза и других методов интеллектуальной деятельности
ИУК-1.2. Выбирает оптимальный вариант решения задачи, аргументируя свой выбор	демонстрирует достаточный уровень оценочных суждений при разборе проблемных профессиональных ситуаций
	умеет получать новые знания на основе анализа, синтеза и других методов, осуществлять поиск информации и решений на основе экспериментальных действий
	владеет навыками выявления научных проблем и использования адекватных методов для их решения
ОПК-7 Способен взаимодействовать с участниками образовательных отношений в рамках реализации образовательных программ	
ИОПК-7.1. Понимает основные аспекты взаимодействия участников образовательных отношений в рамках реализации образовательных программ	знает закономерности формирования и развития детско-взрослых сообществ, их социально-психологические особенности и закономерности развития детских и подростковых сообществ
	умеет обоснованно выбирать и реализовывать формы, методы и средства взаимодействия с участниками образовательных отношений в рамках реализации образовательных программ
	техниками и приемами взаимодействия с участниками образовательных отношений в рамках реализации образовательных программ
ИОПК-7.2. Применяет методы взаимодействия участников образовательных отношений в рамках реализации образовательных программ	знает психолого-педагогические закономерности, принципы, особенности, этические и правовые нормы взаимодействия с участниками образовательных отношений в рамках реализации образовательных программ
	умеет предупреждать и продуктивно разрешать межличностные конфликты
	владеет приемами предупреждения и продуктивного разрешения межличностных конфликтов
ПК-2 Способен применять знания информатики при реализации образовательного процесса	
ИПК 2.1 Владеет предметным содержанием в соответствии с дидактическими целями и возрастными особенностями учащихся	знает перечень и содержательные характеристики учебной документации по вопросам организации и реализации образовательного процесса (примерные программы, основные учебники по предмету); теорию и технологии учета возрастных особенностей студентов
	умеет критически анализировать учебные материалы предметной области с точки зрения их научности, психолого-педагогической и методической целесообразности использования с учетом возрастных особенностей обучающихся
	владеет навыками конструирования предметного содержания и адаптации его в соответствии с возрастными особенностями целевой аудитории
ИПК 2.2 Выбирает вариативное содержания предмета с учетом взаимосвязи урочной и внеурочной форм обучения	знает приоритетные направления развития образовательной системы РФ, требования примерных образовательных программ по учебному предмету
	умеет конструировать содержание обучения в соответствии с уровнем развития научного знания и формой обучения
	владеет навыками разработки рабочих программ по предмету на основе примерных основных общеобразовательных программ и обеспечения ее реализации в соответствии с выбранной формой обучения
ПК-3 Способен организовать деятельность обучающихся, направленную на развитие интереса к информатике в рамках урочной и внеурочной деятельности	
ИПК 3.1 Организует учебную деятельность на уроке, с целью развития интереса у учащихся к предмету	знает основные подходы, принципы, виды и приемы современных педагогических технологий, направленные на развития интереса у учащихся к предмету

Код и наименование индикатора*	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
	умеет использовать достижения отечественной и зарубежной методической мысли, современных методических направлений и концепций с целью развития интереса у учащихся к предмету
	владеет навыками организации учебной деятельности на уроке, развивающей интерес у учащихся к предмету
ИПК 3.2 Организует различные виды внеурочной деятельности, направленные на развитие и поддержание познавательного интереса учащихся	знает условия выбора и приемы использования современных образовательных технологий для повышения мотивации школьников к учебной и учебно-исследовательской работе во внеурочной деятельности по математике и информатике
	умеет организовывать самостоятельную деятельность учащихся, в том числе исследовательскую, направленную на развитие и поддержание познавательного интереса
	имеет навыки использования разнообразных форм, приемов, методов и средств обучения, в том числе по индивидуальным учебным планам, для поддержания познавательного интереса во внеурочной деятельности

2 Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зачётных ед. (108 часов), их распределение по видам работ представлено в таблице

Вид учебной работы		Всего часов	Семестры
			3
Контактная работа, в том числе:		54,3	54,3
Аудиторные занятия (всего) :		50	50
Занятия лекционного типа		24	24
Занятия семинарского типа (семинары, практические занятия)		-	-
Лабораторные занятия		26	26
Иная контактная работа:		4,3	4,3
Контроль самостоятельной работы (КСР)		4	4
Промежуточная аттестация (ИКР)		0,3	0,3
Самостоятельная работа (всего)		53,7	53,7
В том числе:			
Курсовая работа (подготовка и написание)		-	-
Проработка учебного (теоретического) материала		17	17
Выполнение индивидуальных заданий (подготовка сообщений, презентаций) и домашних заданий		10	10
Подготовка к текущему контролю		-	-
Контроль :		26,7	26,7
Подготовка к экзамену		26,7	26,7
Общая трудоемкость	час.	108	108
	в том числе контактная работа	54,3	54,3
	зач. ед	3	3

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины.

№	Наименование разделов (тем)	Количество часов		
		Всего	Аудиторная работа	Внеаудиторная работа

			Л	ПЗ	ЛР	СРС
1	Теоретические основы кибербезопасности	20	8		6	6
2	Технологии защиты информации	30	10		10	10
3	Управление безопасностью и правовые аспекты	26	6		10	10
	ИТОГО по разделам дисциплины	76	24		26	26
	Контроль самостоятельной работы (КСР)	4				4
	Промежуточная аттестация (ИКР)	0,3				0,3
	Подготовка к текущему контролю	-				-
	Подготовка к экзамену (контроль)					26,7
	Общая трудоемкость по дисциплине	108	24		26	58

Примечание: ЛК – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, КСР – контроль самостоятельной работы, СР – самостоятельная работа студента, ИКР – иная контактная работа.

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Теоретические основы кибербезопасности	Лекции №1-2. Введение в кибербезопасность: основные понятия (угрозы, уязвимости, риски), CIA-триада. История развития кибербезопасности. Лекция №3. Классификация кибератак: DoS/DDoS, фишинг, вирусы, трояны, руткиты. Социальная инженерия: методы и защита. Лекция №4. Основы криптографии: симметричное (AES) и асимметричное (RSA) шифрование, хеширование (SHA-256), цифровые подписи. Криптографические протоколы: SSL/TLS, VPN, PGP.	Т
2	Технологии защиты информации	Лекция №5-6. Защита сетей: межсетевые экраны (фаерволлы), системы IDS/IPS, принципы сегментации. Безопасные протоколы: WPA3, SSH, IPSec. Защита Wi-Fi сетей. Лекция №7. Безопасность ОС: харденинг Windows/Linux, управление обновлениями, контроль доступа. Лекция №8. Защита данных: методы резервного копирования, стеганография, безопасное удаление данных. Лекция №9. Антивирусные технологии: принципы работы антивирусов, EDR-системы, анализ вредоносного ПО, sandboxing.	Т
3	Управление безопасностью и правовые аспекты	Лекция №10. Стандарты информационной безопасности: ISO 27001, NIST, PCI DSS. Процесс сертификации. Лекция №11. Правовые аспекты: GDPR, 152-ФЗ, ответственность за нарушения. Этичный хакинг и bug bounty. Лекция №12. Инцидент-менеджмент: этапы реагирования, документооборот, разбор реальных инцидентов (WannaCry, SolarWinds).	Т

Примечание: УП – устный (письменный) опрос, Т – тестирование, КР – контрольная работа, Э – эссе, К – коллоквиум; ПР – практическая работа.

2.3.2 Занятия семинарского типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Теоретические основы кибербезопасности	Семинар №1-2. Анализ реальных кибератак: разбор кейсов (WannaCry, SolarWinds). Практическая работа с инструментами анализа угроз (Maltego). Семинар №3. Криптографические методы: создание и взлом простых шифров, работа с OpenSSL. Практическое применение хеш-функций.	УП, ПР
2	Технологии защиты информации	Семинар №4-5. Настройка межсетевых экранов (iptables, Windows Firewall). Работа с системами обнаружения вторжений (Snort).	УП, ПР

		Семинар №6. Аудит безопасности беспроводных сетей: использование Aircrack-ng, Wireshark. Семинар №7. Харденинг ОС: практическое применение базовых техник защиты Windows/Linux. Семинар №8. Анализ вредоносного ПО в sandbox-среде (Cuckoo Sandbox).	
3	Управление безопасностью и правовые аспекты	Семинар №9-10. Разработка политик информационной безопасности. Практикум по ISO 27001. Семинар №11. Моделирование инцидентов и отработка процедур реагирования. Семинар №12. Юридические кейсы: разбор ситуаций по GDPR и 152-ФЗ. Семинар №13. Деловая игра "Киберучения": командное решение комплексной задачи по защите инфраструктуры.	УП, ПР

Примечание: УП – устный (письменный) опрос, ПР – практическая работа

2.3.3 Лабораторные занятия

Лабораторные занятия не предусмотрены учебным планом.

2.3.4 Примерная тематика курсовых работ

Курсовые работы не предусмотрены учебным планом.

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

№	Вид СР	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
3	Подготовка к выполнению и защите практических работ	1. Белоус, А. И. Основы кибербезопасности : стандарты, концепции, методы и средства обеспечения : [16+] / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 482 с. : схем., ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=617523 (дата обращения: 13.06.2025). – ISBN 978-5-94836-612-8. – Текст : электронный. 2. Ванина, А. Г. Персональная кибербезопасность : учебное пособие (курс лекций) : направление подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) : [16+] / А. Г. Ванина, Д. В. Орёл, С. В. Аникуев ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2022. – 138 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=712359 (дата обращения: 13.06.2025). – Библиогр. в кн. – Текст : электронный. 3. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313 (дата обращения: 13.06.2025). 4. Информатика : учебник для вузов — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 752 с. — (Высшее образование). — ISBN 978-5-534-20227-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568691 (дата обращения: 10.06.2025).
4	Подготовка к тестированию (текущей аттестации)	1. Белоус, А. И. Основы кибербезопасности : стандарты, концепции, методы и средства обеспечения : [16+] / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 482 с. : схем., ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=617523 (дата обращения: 13.06.2025). – ISBN 978-5-94836-612-8. – Текст : электронный. 2. Ванина, А. Г. Персональная кибербезопасность : учебное пособие (курс лекций) : направление подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) : [16+] / А. Г. Ванина, Д. В. Орёл, С. В. Аникуев ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2022. – 138 с. : ил., табл.

		– Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=712359 (дата обращения: 13.06.2025). – Библиогр. в кн. – Текст : электронный. 3. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313 (дата обращения: 13.06.2025). 4. Информатика : учебник для вузов — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 752 с. — (Высшее образование). — ISBN 978-5-534-20227-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568691 (дата обращения: 10.06.2025).
--	--	--

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,

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 дополнен и конкретизирован в зависимости от контингента обучающихся.

3 Образовательные технологии, применяемые при освоении дисциплины

С целью формирования и развития профессиональных навыков обучающихся, в соответствии с требованиями ФГОС ВО по направлению подготовки, для реализации компетентностного подхода программа предусматривает широкое использование в учебном процессе следующих форм учебной работы:

- активные формы (лекция, вводная лекция, обзорная лекция, заключительная лекция, презентация);
- интерактивные формы (практическое занятие, семинар, компьютерная симуляция, коллоквиум);
- внеаудиторные формы (консультация, практикум, самостоятельная работа, подготовка реферата, написание курсовой работы);
- формы контроля знаний (групповой опрос, контрольная работа, практическая работа, тестирование, коллоквиум, зачёт, экзамен).

3.1 Образовательные технологии при проведении лекций

Лекция – одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала. Она предшествует всем другим формам организации учебного процесса, позволяет оперативно актуализировать учебный материал дисциплины. Для повышения эффективности лекций целесообразно воспользоваться следующими рекомендациями:

- четко и ясно структурировать занятие;
- рационально дозировать материал в каждом из разделов;
- использовать простой, доступный язык, образную речь с примерами и сравнениями;
- отказаться, насколько это возможно, от иностранных слов;
- использовать наглядные пособия, схемы, таблицы, модели, графики и т. п.;

- применять риторические и уточняющие понимание материала вопросы;
- обращаться к техническим средствам обучения.

№	Тема	Виды применяемых образовательных технологий	Кол. час
1	Теоретические основы кибербезопасности	Аудиовизуальная технология. Репродуктивная технология. Использование средств мультимедиа.	6+2*
2	Технологии защиты информации	Аудиовизуальная технология. Репродуктивная технология. Лекции с проблемным изложением. Эвристическая беседа. Использование средств мультимедиа.	6+4*
3	Управление безопасностью и правовые аспекты	Аудиовизуальная технология. Репродуктивная технология. Лекции с проблемным изложением. Эвристическая беседа. Использование средств мультимедиа.	2+4*
Итого по курсу			24
в том числе интерактивное обучение*			10*

Аудиовизуальная технология – основная информационная технология обучения, осуществляемая с использованием носителей информации, предназначенных для восприятия человеком по двум каналам одновременно зрительному и слуховому при помощи соответствующих технических устройств, а также закономерностей, принципов и особенностей представления и восприятия аудиовизуальной информации.

3.2 Образовательные технологии при проведении практических занятий

Практическое (семинарское) занятие – основная интерактивная форма организации учебного процесса, дополняющая теоретический курс или лекционную часть учебной дисциплины и призванная помочь обучающимся освоиться в «пространстве» дисциплины; самостоятельно оперировать теоретическими знаниями на конкретном учебном материале. Для практического занятия в качестве темы выбирается обычно такая учебная задача, которая предполагает не существенные эвристические и аналитические напряжения и продвижения, а потребность обучающегося «потрогать» материал, опознать в конкретном то общее, о чем говорилось в лекции

№	Тема	Виды применяемых образовательных технологий	Кол. час
1	Теоретические основы кибербезопасности	Проектная деятельность. Репродуктивная технология. Использование средств мультимедиа. Работа в малых группах.	4+2*
2	Технологии защиты информации	Проектная деятельность. Репродуктивная технология. Использование средств мультимедиа. Работа в малых группах.	6+4*
3	Управление безопасностью и правовые аспекты	Проектная деятельность. Репродуктивная технология. Использование средств мультимедиа. Работа в малых группах.	6+2*
Итого по курсу			26
в том числе интерактивное обучение*			8*

4 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Практикум по решению задач на ЭВМ». Оценочные средства включает контрольные материалы для проведения **текущего контроля** в формах вопросов устного опроса (У), тестовых заданий (Т), заданий для практической работы (П) и **промежуточной аттестации** в форме вопросов к зачету (З). 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.

4.1 Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	Теоретические основы кибербезопасности	УК-1, ОПК-7, ПК-2, ПК-3	Задания практических работ Тестовые задания	Экзамен
2	Технологии защиты информации	УК-1, ОПК-7, ПК-2, ПК-3	Задания практических работ Тестовые задания	Экзамен
3	Управление безопасностью и правовые аспекты	УК-1, ОПК-7, ПК-2, ПК-3	Задания практических работ Тестовые задания	Экзамен

4.2 Показатели, критерии и шкала оценки сформированных компетенций

Продвинутый уровень – полная сформированность и устойчивость всех компетенций, охваченных компетентностной моделью.

Базовый уровень – прочная сформированность и устойчивость компетенций, охваченных компетентностной моделью.

Пороговый уровень – достаточная (фрагментарная) сформированность компетенций, охваченных компетентностной моделью.

Код и наименование компетенций	Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания		
	пороговый	базовый	продвинутый

	оценка		
	зачтено	зачтено	зачтено
ПК-1	Знает - сформированы необходимые знания по каждой компетенции.	Знает - сформированы прочные и глубокие знания по каждой компетенции.	Знает - сформированы полные, глубокие и систематические знания по каждой компетенции.
	Умеет - достигнут приемлемый уровень умений применять полученные знания на практике.	Умеет - достигнут достаточный уровень умений применять полученные знания на практике.	Умеет - достигнут высокий уровень умений применять полученные знания на практике
	Владеет - продемонстрировано владение навыками применения полученных знаний и умений в профессиональной деятельности	Владеет - продемонстрировано владение навыками применения полученных знаний и умений в профессиональной деятельности.	Владеет - продемонстрировано владение широким спектром навыков применения полученных знаний и умений в профессиональной деятельности

4.3 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

Примерные вопросы для устного опроса

1. Объясните принципы CIA-триады и приведите примеры их нарушения в реальных кибератаках.
2. В чем разница между угрозой, уязвимостью и риском в контексте информационной безопасности?
3. Какие основные типы вредоносного ПО вы знаете? Кратко охарактеризуйте каждый.
4. Объясните, как работает фишинговая атака и как можно ее распознать.
5. Что такое социальная инженерия? Приведите пример атаки с ее использованием.
6. Опишите различия между симметричным и асимметричным шифрованием.
7. Для чего используется хеширование? Назовите популярные алгоритмы хеширования.
8. Как работает механизм цифровой подписи?
9. Объясните назначение и принцип работы SSL/TLS протокола.
10. Что такое VPN и какие технологии защиты он использует?
11. Какие существуют методы аутентификации? Сравните их эффективность.
12. Объясните принцип работы межсетевого экрана (фаервола).
13. В чем разница между IDS и IPS системами?
14. Какие существуют способы защиты беспроводных сетей?
15. Что такое "харденинг ОС" и какие основные меры он включает?
16. Опишите принцип работы антивирусных программ.
17. Что такое sandbox и как он используется в кибербезопасности?
18. Какие существуют методы резервного копирования данных?
19. Объясните принцип "минимальных привилегий" и его значение для безопасности.
20. Что такое инцидент информационной безопасности и какова типичная процедура реагирования?
21. Какие основные положения содержит закон 152-ФЗ "О персональных данных"?
22. В чем суть GDPR и как он влияет на российские компании?
23. Что такое этичный хакинг и bug bounty программы?
24. Опишите стандарт ISO 27001 и его значение для организаций.
25. Какие существуют методы защиты от DDoS-атак?
26. Что такое АPT-атаки и чем они отличаются от обычных кибератак?
27. Объясните понятие "нулевого дня" (zero-day) в контексте уязвимостей.
28. Какие существуют методы защиты от SQL-инъекций?
29. Что такое криптовалюты с точки зрения безопасности? Какие угрозы с ними связаны?

Примерные тестовые задания для текущей аттестации

Тестовые задания раздел №1

(Указать один правильный ответ)

1. Что включает CIA-триада в кибербезопасности?

1. Конфиденциальность, Интеграция, Доступность
2. **Конфиденциальность, Целостность, Доступность**
3. Кодирование, Инженерия, Аутентификация
4. Криптография, Идентификация, Авторизация

2. Какая атака направлена на перегрузку ресурсов системы?

1. Фишинг
2. **DoS-атака**
3. SQL-инъекция
4. Кросс-сайт скриптинг

3. Какой вид вредоносного ПО шифрует данные и требует выкуп?

1. Троян
2. Черви
3. **Рансомвер**
4. Спам

4. Что такое фишинг?

1. Атака через перехват паролей в сети
2. **Мошенничество с целью кражи данных через поддельные письма/сайты**
3. Взлом Wi-Fi-сетей
4. Заражение через USB-носители

5. Какой протокол обеспечивает безопасную передачу данных в интернете?

1. HTTP
2. FTP
3. **HTTPS**
4. SMTP

6. Что проверяет цифровая подпись?

1. Скорость передачи данных
2. **Целостность и аутентичность данных**
3. Доступность сервера
4. Шифрование файлов

7. Как называется защитный механизм, фильтрующий сетевой трафик?

1. **Фаервол**
2. VPN
3. SSH
4. IDS

8. Какой стандарт описывает лучшие практики информационной безопасности?

1. **ISO 27001**
2. IEEE 802.11
3. TCP/IP
4. HTML5

9. Что такое социальная инженерия?

1. Разработка ПО для защиты данных
2. **Методы манипуляции людьми для получения информации**
3. Шифрование сообщений
4. Анализ сетевого трафика

10. Какой алгоритм относится к асимметричному шифрованию?

1. AES
 2. **RSA**
 3. SHA-256
 4. MD5
- 11. Для чего используется VPN?**
1. Ускорение интернет-соединения
 2. **Безопасный удалённый доступ к сети**
 3. Сканирование портов
 4. Блокировка рекламы
- 12. Что такое SQL-инъекция?**
1. Заражение через USB
 2. **Внедрение вредоносного кода в запросы к БД**
 3. Атака на маршрутизаторы
 4. Кража cookies
- 13. Какой инструмент обнаруживает вторжения в сеть?**
1. **IDS (Intrusion Detection System)**
 2. FTP-сервер
 3. Брандмауэр Windows
 4. DHCP
- 14. Что проверяет аудит безопасности?**
1. **Соответствие системы политикам защиты**
 2. Скорость интернета
 3. Количество пользователей
 4. Работу антивируса
- 15. Какой закон РФ регулирует защиту персональных данных?**
1. **152-ФЗ**
 2. 161-ФЗ
 3. 149-ФЗ
 4. 187-ФЗ
- 16. Что такое двухфакторная аутентификация (2FA)?**
1. **Использование двух методов проверки личности**
 2. Двойное шифрование данных
 3. Два пароля для входа
 4. Резервное копирование
- 17. Как называется тестирование на проникновение?**
1. **Penetration Testing**
 2. Data Mining
 3. Stress Testing
 4. Code Review
- 18. Какой алгоритм хеширования считается устаревшим?**
1. **MD5**
 2. SHA-256
 3. AES
 4. RSA
- 19. Что защищает принцип "минимальных привилегий"?**
1. **Предоставление прав только по необходимости**
 2. Шифрование всех данных
 3. Автоматические обновления
 4. Блокировку USB
- 20. Какой термин описывает исправление уязвимости?**
1. **Патч**
 2. Бэкдор
 3. Эксплойт
 4. Фарминг

21. Что такое ботнет?

1. Сеть заражённых устройств под управлением злоумышленника
2. Защищённый сервер
3. Виртуальная частная сеть
4. Система обнаружения вторжений

22. Какой протокол НЕбезопасен для передачи паролей?

1. FTP
2. SSH
3. HTTPS
4. SFTP

23. Что такое zero-day уязвимость?

1. Уязвимость, для которой нет заплатки
2. Атака в полночь
3. Ошибка в антивирусе
4. Устаревший алгоритм шифрования

24. Какой метод защиты предотвращает подделку email?

1. SPF/DKIM
2. VPN
3. CAPTCHA
4. BIOS-пароль

25. Как называется вредоносное ПО, скрывающееся в системе?

1. Руткит
2. Файрвол
3. Троян
4. Шифровальщик

Примерные задания для практических работ

На самостоятельную работу планируется выполнение индивидуального варианта по образцу задания проделанного на занятиях.

1. **Фишинг-анализ:** Исследуйте подозрительное email-сообщение (предоставленное преподавателем) и определите признаки фишинга.
2. **Социальная инженерия:** Разработайте сценарий телефонного вишинга и предложите методы защиты от него.
3. **Шифрование данных:** Зашифруйте текст с помощью OpenSSL (AES-256), затем расшифруйте его.
4. **Хеширование:** Сравните скорость и коллизии для MD5, SHA-1 и SHA-256 на заданном наборе данных.
5. **Цифровая подпись:** Создайте ключевую пару RSA, подпишите документ и проверьте подлинность подписи.
6. **Настройка фаервола:** Создайте правила для iptables (Linux) или Windows Firewall, блокирующие нежелательный трафик.
7. **Анализ сетевого трафика:** Используя Wireshark, выявите подозрительную активность в предоставленном дампе трафика.
8. **Аудит Wi-Fi:** С помощью Aircrack-ng проанализируйте безопасность беспроводной сети (в учебных целях).
9. **IDS/IPS:** Настройте Snort для обнаружения аномального трафика (например, сканирования портов).
10. **VPN:** Разверните VPN-сервер (OpenVPN/WireGuard) и проверьте его работу.
11. **Харденинг Windows:** Отключите ненужные службы, настройте политики паролей и аудит событий.
12. **Харденинг Linux:** Настройте SELinux/AppArmor, ограничьте права пользователей.
13. **Анализ вредоносного ПО:** Исследуйте образец malware в песочнице (Cuckoo Sandbox или Any.Run).

14. **Антивирусный аудит:** Проверьте систему с помощью AVZ или Kaspersky Virus Removal Tool, проанализируйте отчет.
15. **Уязвимости веб-приложений:** Найдите и эксплуатируйте SQL-инъекцию в учебном стенде (например, DVWA).
16. **Резервное копирование:** Настройте автоматическое резервирование данных с помощью BorgBackup или Veeam.
17. **Инцидент-менеджмент:** Разработайте план реагирования на утечку данных (на основе предоставленного кейса).
18. **Аудит по ISO 27001:** Проведите проверку учебной системы на соответствие требованиям стандарта.
19. **GDPR-анализ:** Оцените, какие данные в учебной базе являются персональными по GDPR, и предложите меры защиты.
20. **Киберучения:** В командах смоделируйте атаку и защиту инфраструктуры (например, с помощью MITRE ATT&CK).

4.1.4 Зачетно-экзаменационные материалы для промежуточной аттестации

Примерные экзаменационные вопросы

1. CIA-триада: раскройте компоненты (конфиденциальность, целостность, доступность) и приведите примеры их реализации в корпоративной среде.
2. Классификация угроз информационной безопасности: внутренние vs внешние, преднамеренные vs случайные. Примеры для каждого типа.
3. Сравнительный анализ вирусов, червей, троянов и руткитов. Механизмы их распространения и защиты.
4. Фишинг и его разновидности (таргетированный, spear phishing). Методы идентификации фишинговых атак.
5. Принципы работы социальной инженерии. Разбор реального кейса (на выбор экзаменуемого).
6. Криптографические методы защиты информации: симметричные и асимметричные алгоритмы. Сравнение AES и RSA.
7. Цифровые подписи и сертификаты: схема работы, применение в электронном документообороте.
8. Протокол SSL/TLS: этапы установления защищенного соединения, виды атак на протокол.
9. VPN-технологии: принципы работы, сравнение IPsec и OpenVPN, уязвимости.
10. Многофакторная аутентификация: методы реализации, преимущества перед однофакторной.
11. Межсетевые экраны: архитектура, типы (пакетные, stateful), правила настройки.
12. Системы обнаружения и предотвращения вторжений: сравнение IDS и IPS, примеры реализации.
13. Безопасность беспроводных сетей: анализ уязвимостей WEP, WPA, WPA2 и методов защиты.
14. Харденинг операционных систем: пошаговая методика для Windows/Linux.
15. Антивирусные системы: принципы работы, методы обнаружения вредоносного кода, ограничения.
16. Технологии sandboxing: применение для анализа вредоносного ПО, примеры реализаций.
17. Стратегии резервного копирования: полное/инкрементальное/дифференциальное копирование, схемы ротации.
18. Принцип наименьших привилегий: реализация в ОС и приложениях, значение для безопасности.
19. Управление инцидентами информационной безопасности: этапы обработки, роль CSIRT.

20. Законодательная база РФ в области ИБ: 152-ФЗ, 187-ФЗ, требования к операторам персональных данных.
21. GDPR: ключевые положения, отличие от 152-ФЗ, последствия нарушений.
22. Этический хакинг: методики тестирования на проникновение, правовые аспекты.
23. Стандарт ISO 27001: структура, процесс внедрения, преимущества сертификации.
24. Защита от DDoS-атак: классификация атак, методы фильтрации трафика.
25. АPT-атаки: характерные признаки, этапы проведения, методы противодействия.
26. Zero-day уязвимости: механизмы эксплуатации, стратегии защиты.
27. Инъекционные атаки: SQL-инъекции, XSS, методы защиты веб-приложений.
28. Блокчейн и безопасность: анализ уязвимостей криптовалютных систем.
29. IoT-безопасность: типовые угрозы и методы защиты "умных" устройств.
30. Современные тренды кибербезопасности: ИИ в защите систем, квантовые вычисления, биометрические технологии.

5 Перечень учебной литературы, информационных ресурсов и технологий

5.1 Учебная литература

1. Белоус, А. И. Основы кибербезопасности : стандарты, концепции, методы и средства обеспечения : [16+] / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 482 с. : схем., ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=617523> (дата обращения: 13.06.2025). – ISBN 978-5-94836-612-8. – Текст : электронный.

2. Ванина, А. Г. Персональная кибербезопасность : учебное пособие (курс лекций) : направление подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) : [16+] / А. Г. Ванина, Д. В. Орёл, С. В. Аникуев ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2022. – 138 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=712359> (дата обращения: 13.06.2025). – Библиогр. в кн. – Текст : электронный.

3. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561313> (дата обращения: 13.06.2025).

4. Информатика : учебник для вузов — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 752 с. — (Высшее образование). — ISBN 978-5-534-20227-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/568691> (дата обращения: 10.06.2025).

5.2 Периодические издания

1. Базы данных компании «Ист Вью». - <http://dlib.eastview.com>
2. Электронная библиотека GREBENNICON.RU. - <https://grebennikon.ru/>
3. Методические вопросы преподавания инфокоммуникаций в высшей школе. - URL: <http://elibrary.ru/contents.asp?titleid=55718>
4. Вестник Волгоградского государственного университета. Серия 1. Математика. Физика. (Математическая физика и компьютерное моделирование) – URL: http://biblioclub.ru/index.php?page=journal_red&jid=279797
5. Вестник Воронежского государственного университета. Серия: Физика. Математика. – URL: <http://elibrary.ru/contents.asp?titleid=9761>
6. Математика в высшем образовании. - URL: https://e.lanbook.com/journal/2368#journal_name
7. Инновации на основе информационных и коммуникационных технологий. - URL: <http://elibrary.ru/contents.asp?issueid=1438371>.

8. Математика и ее приложения. Журнал Ивановского математического общества. – URL: http://elibrary.ru/title_about.asp?id=32863
9. Математические заметки СВФУ. Научно-исследовательский институт математики Северо-Восточного федерального университета им. М.К. Аммосова (Якутск). – URL: <http://elibrary.ru/contents.asp?issueid=1443590>
10. Математические методы и модели: теория, приложения и роль в образовании. Ульяновский государственный технический университет (Ульяновск). – URL: <https://elibrary.ru/contents.asp?titleid=54645>
11. Математические труды. Институт математики им. С.Л. Соболева СО РАН (Новосибирск). – URL: <http://elibrary.ru/contents.asp?issueid=1389771>
12. Математический вестник педвузов и университетов Волго-Вятского региона (Киров). – URL: <https://elibrary.ru/contents.asp?titleid=28395>
13. Информатика, вычислительная техника и инженерное образование. URL: <http://elibrary.ru/contents.asp?issueid=1567393>
14. Математическое образование. Фонд математического образования и просвещения (Москва). – URL: <http://elibrary.ru/contents.asp?issueid=1408321>

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

Электронно-библиотечные системы (ЭБС)

1. ЭБС «Университетская библиотека онлайн» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы; коллекция медиа-материалов: аудиокниги, аудиофайлы, видеокурсы, экспресс-подготовка к экзаменам, презентации, тесты, карты, онлайн-энциклопедии, словари]. – URL: <http://www.biblioclub.ru/>.
2. ЭБС «ZnaniUM» [учебные, научные, справочные, научно-популярные издания различных издательств, журналы]. – URL: <https://znanium.ru/>.
3. ЭБС «Лань» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы]. – URL: <http://e.lanbook.com/>.
4. Образовательная платформа «Юрайт» [учебники и учебные пособия издательства «Юрайт», медиа-материалы, тесты]. – URL: <https://urait.ru/>.
5. ЭБС «BOOK.ru» [учебная литература, журналы]. – URL: <https://www.book.ru>.
6. ЭБс ОИЦ «Академия» [учебные издания по общеобразовательным дисциплинам СПО для первого курса, включенных в ФПУ]. – URL: <https://academia-moscow.ru/elibrary/>.

Профессиональные базы данных

1. Виртуальный читальный зал Российской государственной библиотеки (РГБ). – URL: <https://ldiss.rsl.ru/>.
2. Национальная электронная библиотека (НЭБ) [включает Электронную библиотеку диссертаций РГБ] : [федеральная государственная информационная система Министерства культуры РФ]. – URL: <https://rusneb.ru/> (*полный доступ к объектам НЭБ – в локальной сети с компьютеров библиотеки филиала*).
3. Научная электронная библиотека «eLIBRARY.RU» [русские научные журналы, труды конференций; Российская национальная база данных научного цитирования (РИНЦ)]. – URL: <http://www.elibrary.ru/>.
4. Универсальные базы данных «ИВИС» [русские научные журналы по вопросам педагогики и образования, экономики и финансов, информационным технологиям, экономике и предпринимательству, общественным и гуманитарным наукам, индивидуальные издания, Вестники МГУ, СПбГУ, статистические издания России и стран СНГ]. – URL: <https://eivis.ru/basic/details>.
5. Полнотекстовая коллекция журналов на платформе РЦНИ. Национальная платформа периодических научных изданий. – URL: <https://journals.rcsi.science/>.
6. Общероссийский портал «Math-Net.Ru» : информационная система доступа к научной информации по математике, физике, информационным технологиям и смежным

наукам / Математический институт имени В. А. Стеклова РАН. – URL: <http://www.mathnet.ru/>.

7. Президентская библиотека им. Б.Н. Ельцина. – URL: <https://www.prilib.ru/>.

8. Журналы издательства Wiley: [полнотекстовая коллекция электронных журналов по: химии, физике, математике, социальным и гуманитарным наукам, психологии, бизнесу, экономике и юриспруденции]. – URL: <https://onlinelibrary.wiley.com/>.

9. Полнотекстовая коллекция книг eBook Collections издательства SAGE Publications: [включает монографии и справочники по различным областям знаний: бизнес, психология, криминология и уголовное право, образование, география, науки о Земле и окружающей среде, здравоохранение и социальная помощь, СМИ и коммуникация, культурология, политика и международные отношения, социология и др.]. – URL: <https://sk.sagepub.com/books/discipline>.

10. Ресурсы Springer Nature: [Полнотекстовая коллекция книг (монографий) издательств Springer Nature по различным отраслям знаний]. – URL: <https://link.springer.com/>, <https://www.nature.com/>.

Информационные справочные системы

1. КонсультантПлюс : справочная правовая система (*доступ – в локальной сети с компьютеров библиотеки филиала*).

Ресурсы свободного доступа

1. Официальный интернет-портал правовой информации. Государственная система правовой информации. – URL: <http://pravo.gov.ru/>

2. КонсультантПлюс : некоммерческая интернет-версия справочной правовой системы. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=home&utm_csource=online&utm_cmedium=button.

3. Министерство науки и высшего образования Российской Федерации (Минобрнауки России) - официальный сайт. – URL: <https://www.minobrnauki.gov.ru>

4. Министерство просвещения Российской Федерации - официальный сайт. – URL: <https://edu.gov.ru>

5. Портал «Культура.РФ» : гуманитарный просветительский проект, посвященный культуре России [кино, музеи, музыка, театры, архитектура, литература, персоны, традиции, лекции-онлайн] : сайт / Министерство культуры РФ. – URL: <https://www.culture.ru/>.

6. Справочно-информационный портал «Грамота.ру» / Министерство цифрового развития, связи и массовых коммуникаций РФ. – URL: <http://www.gramota.ru/>.

7. Лекториум [раздел «Медiateка» – открытый видеоархив лекций на русском языке]: образовательная платформа : сайт. – URL: <https://www.lektorium.tv/medialibrary>.

8. Научная электронная библиотека «КиберЛенинка» [русские научные журналы]. – URL: <http://cyberleninka.ru/>.

9. Большая российская энциклопедия: [электронная версия] / Министерство культуры РФ. – URL: <https://bigenc.ru/>.

10. Лингвистический проект «СЛОВАРИ.РУ» / Институт русского языка им. В. В. Виноградова РАН. – URL: <http://slovari.ru/start.aspx?s=0&p=3050>.

Собственные электронные образовательные и информационные ресурсы

1. База информационных потребностей [КубГУ и филиалов] (*разделы: Научные публикации преподавателей и обучающихся; Информация об участии преподавателей и обучающихся в научных конференциях; Темы выпускных квалификационных работ студентов*). – URL: <https://infoneeds.kubsu.ru/infoneeds/>.

2. Электронная библиотека информационных ресурсов филиала [КубГУ в г. Славянске-на-Кубани]. – URL: <http://sgpi.ru/bip.php>.

3. Поступления литературы в библиотеки филиалов : [электронный каталог библиотек филиалов КубГУ]. – URL: <http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=1>.

4. Электронная библиотека трудов учёных КубГУ. – URL: <http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=6>.

6 Методические указания для студентов по освоению дисциплины

6.1 Общие рекомендации по самостоятельной работе обучающихся

При изучении дисциплины «Практикум по решению задач на ЭВМ» студенты часть материала должны проработать самостоятельно. Роль самостоятельной работы велика.

Планирование самостоятельной работы студентов по дисциплине «Практикум по решению задач на ЭВМ» необходимо проводить в соответствии с уровнем подготовки студентов к изучаемой дисциплине.

Методические указания к лекционным занятиям

Самостоятельная работа студентов распадается на два самостоятельных направления: на изучение и освоение теоретического лекционного материала, и на освоение методики решения практических задач.

При всех формах самостоятельной работы студент может получить разъяснения по непонятным вопросам у преподавателя на индивидуальных консультациях в соответствии с графиком консультаций. Студент может также обратиться к рекомендуемым преподавателем учебникам и учебным пособиям, в которых теоретические вопросы изложены более широко и подробно, чем на лекциях и с достаточным обоснованием.

Консультация – активная форма учебной деятельности в педвузе. Консультацию предваряет самостоятельное изучение студентом литературы по определенной теме. Качество консультации зависит от степени подготовки студентов и остроты поставленных перед преподавателем вопросов.

Для дополнительной проработки лекционного материала студенты могут использовать основную и дополнительную литературу, рекомендуемые источники интернета, компьютерные учебники и дополнительные электронные материалы. Для работы с электронными материалами имеется возможность использования электронных библиотек, компьютеров в читальных залах библиотеки, локальной компьютерной сети ВУЗа.

Методические указания к лабораторным занятиям

Основной частью самостоятельной работы студента является его систематическая подготовка к лабораторным занятиям. Студенты должны быть нацелены на важность качественной подготовки к таким занятиям. При подготовке к лабораторным занятиям студенты должны освоить вначале теоретический материал по новой теме занятия, с тем чтобы использовать эти знания при решении практических задач. Затем просмотреть пояснения к примерам проектов, сделанные преподавателем в описании лабораторной работы, разобраться с примером проекта, приведенными в этом описании. Разработка приведенного проекта и отдельная разработка по образцу индивидуального задания. Если некоторые задания вызвали затруднения при решении, попросить объяснить преподавателя на очередном занятии или консультации.

Для работы на лабораторных занятиях, самостоятельной работы во внеаудиторное время, а также для подготовки к защите проектов рекомендуется использовать методические рекомендации к лабораторным занятиям. При подготовке к тестированию необходимо повторить материал, рассмотренный на лабораторных занятиях, прорешать соответствующие задачи или примеры, убедиться в знании необходимых формул, определений и т. д.

Лабораторные работы выполняются в специализированных классах, оснащенных современными компьютерами и программным обеспечением. Компьютерный класс находится в локальной компьютерной сети с выходом в корпоративную сеть ВУЗа и глобальную сеть Internet. При выполнении и защите лабораторной работы студенты как правило используют метод проектов, который требует дополнительной подготовки студента к его защите, часто используется работа в малых группах.

Методические указания к самостоятельной работе

Ряд вопросов курса отведены для самостоятельной проработки студентами. При этом у лектора появляется возможность расширить круг изучаемых проблем, дать на самостоятельную

проработку новые интересные вопросы. Студент должен разобраться в рекомендуемой литературе и письменно изложить кратко и доступно для себя основное содержание материала. Преподаватель проверяет качество усвоения самостоятельно проработанных вопросов на лабораторных занятиях, защите проектов, тестировании и во время зачета. Затем корректирует изложение материала и нагрузку на студентов.

Для получения практического опыта программирования задач по дисциплине «Практикум по решению задач на ЭВМ» на лабораторных занятиях и для работы во внеаудиторное время предлагается самостоятельная работа над проектами в рамках индивидуальных заданий. Контроль над выполнением проектов и их оценка осуществляется в форме собеседования.

Таким образом, использование всех рекомендуемых видов самостоятельной работы дает возможность значительно активизировать работу студентов над материалом курса и повысить уровень их усвоения.

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.

6.2 Рейтинговая система оценки текущей успеваемости студентов

Распределение рейтинговых баллов по видам оцениваемых работ представлено в следующей таблице.

№	Наименование разделов	Виды оцениваемых работ	Максимальное кол-во баллов
1	Основы Python	Активная работа на занятиях Защита лабораторных работ	1 20
2	Алгоритмы и структуры данных	Активная работа на занятиях Защита лабораторных работ	1 12
3	Файлы, ООП и сложные задачи ЕГЭ	Активная работа на занятиях Защита лабораторных работ	2 24
3	Текущая аттестация по всем разделам	Компьютерное тестирование	40
ВСЕГО			100

6.3 Организация процедуры промежуточной аттестации

Промежуточная аттестация осуществляется в форме зачета и организуется в соответствии с утвержденным рабочим учебным планом, рабочей программой дисциплины и расписанием. Студенты очной формы обучения обязаны сдать зачет до начала экзаменационной сессии. Зачет проводится во время последних аудиторных занятий или в дополнительно назначенное время. Не сдача до начала сессии зачета не является основанием для не допуска к экзаменам. Не сдача зачета является академической задолженностью. Повторная сдача (пересдача) зачета возможна только после окончания экзаменационной сессии в соответствии с утвержденным деканом расписанием пересдач. Форм проведения зачета – устная, письменная и др. – устанавливаются преподавателем и доводятся до сведения студентов в начале семестра.

Освоение материала контролируется в процессе проведения рейтинг - контроля. Контрольные вопросы и задания для проведения текущего контроля выбираются из содержания разделов дисциплины. В соответствии с рейтинговой системой текущий контроль производится регулярно в течение семестра путем балльной оценки качества усвоения теоретического материала (тестирование) и результатов практической деятельности (выполнение индивидуальных заданий и самостоятельных работ). Промежуточная аттестация (зачет) производится в конце семестра также путем балльной оценки. Итоговый рейтинг определяется

суммированием баллов текущей оценки в течение семестра и баллов промежуточной аттестации в конце семестра по результатам зачета. Максимальный итоговый рейтинг соответствует 100 баллам (60 – текущая оценка в семестре, 40 – промежуточная аттестация в конце семестра).

Итоговая оценка учитывает совокупные результаты контроля знаний. Дополнительно может проводиться по вопросам опрос в устной форме. Содержание вопросов приведено выше.

Оценка дополнительного опроса отражается как повышение его баллов до уровня «зачтено», если студент:

- в целом раскрыл содержание материала в области, предусмотренной вопросом;
- изложил материал достаточно грамотным языком в определенной логической последовательности, точно использовал терминологию;
- правильно выполнил рисунки, чертежи, графики, использовал наглядные пособия, соответствующие ответу;
- отвечал практически самостоятельно без значительного числа наводящих вопросов.

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 опросе;
- 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.

7 Материально-техническое обеспечение по дисциплине

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель. Технические средства обучения: проектор, экран, компьютер/ноутбук	Офисное ПО. База учебных планов, учебно-методических комплексов, учебных пособий по предмету

Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель. Технические средства обучения: проектор, экран, компьютер/ноутбук	Офисное ПО. База учебных планов, учебно-методических комплексов, учебных пособий по предмету
Учебные аудитории для проведения лабораторных занятий	Компьютерный класс, оснащенный персональными ЭВМ и соответствующим программным обеспечением (ПО)	Офисное ПО. Системы программирования и разработки приложений. База учебных планов, учебно-методических комплексов, учебных пособий по предмету

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)	Офисное ПО. База учебных планов, учебно-методических комплексов, учебных пособий по предмету
Помещение для самостоятельной работы обучающихся (ауд.20)	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)	Офисное ПО. База учебных планов, учебно-методических комплексов, учебных пособий по предмету
Компьютерный класс для самостоятельной работы обучающихся (ауд.24)	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)	Офисное ПО. База учебных планов, учебно-методических комплексов, учебных пособий по предмету. Системы программирования и разработки приложений.

