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

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«30» май 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.03 ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Специальность 01.05.01 Фундаментальные математика и механика

Направленность (профиль) Вычислительная механика и компьютерный инжиниринг
Фундаментальная математика и ее приложения
Математическое моделирование
Машинное обучение, методы оптимизации и прогнозирование

Форма обучения очная

Квалификация Математик. Механик. Преподаватель

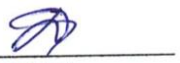
Краснодар 2025

Рабочая программа дисциплины «Цифровая безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности 01.05.01 Фундаментальные математика и механика

Программу составила:
В.В. Василенко, канд. физ.-мат. наук
И.О. Фамилия, должность, ученая степень, ученое звание


подпись

Рабочая программа дисциплины «Цифровая безопасность» утверждена на заседании кафедры Функционального анализа и алгебры
протокол № 11 от «13» мая 2025 г.
Заведующий кафедрой Барсукова В.Ю.
фамилия, инициалы


подпись

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 4 от «14» мая 2025 г.
Председатель УМК факультета Шмалько С.П.
фамилия, инициалы


подпись

Рецензенты:

Савин В.Н., кандидат технических наук, доцент, и.о. зав. кафедрой высшей математики ФГБОУ ВО «Кубанский государственный технологический университет»;

Засядко О.В., кандидат педагогических наук, доцент, доцент кафедры информационных образовательных технологий КубГУ.

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины Курс посвящен изучению формирования цифрового портрета пользователя; принципов и основ защиты информации, в том числе и с административно-правовой стороны; элементов математических основ организации защиты цифровой информации (криптографические способы, основы стеганографии); освоению навыков применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; формированию компетенций в области организации многоуровневой сетевой защиты.

1.2 Задачи дисциплины

Освоить принципы цифровой гигиены данных, профилактику сетевых угроз, основные инструменты и технологии защиты данных. Сформировать практические навыки распознавания атак и угроз стабильности передачи и целостности информации, защиты цифровых данных в сети.

1.3 Место дисциплины (модуля) в структуре образовательной программы

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

Дисциплине предшествуют дисциплины: Дискретная математика, Теория чисел, Фундаментальная и компьютерная алгебра, Использование свободных и отечественных операционных систем, Основы компьютерных наук. Дисциплина может быть рассмотрена как надстройка (обобщающая часть) дисциплины Информационная безопасность.

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

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

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ОПК-5 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	
ОПК-5.1. Алгоритмизирует задачи на основе существующих методов и стандартных решений при разработке компьютерных программ	**Знает** основные стандарты и принципы информационной безопасности, понятия цифровой безопасности; **Умеет** распознавать угрозы стабильной работы в сети, планировать многоуровневую защиту данных, применять методы анализа для выявления уязвимых позиций в программном и аппаратном обеспечении электронно-вычислительных устройств; **Владеет** навыками работы по обнаружению и защите от атак различного вида на цифровую информацию с использованием современного программного обеспечения.
ОПК-5.2. Реализует алгоритмы с использованием современных средств разработки прикладного программного обеспечения	**Знает** основы криптографической защиты информации, принципы стеганографии и классические алгоритмы шифрования, расшифрования и признаки дешифрования; **Умеет** анализировать цифровые данные и распознавать наличие потока зашифрованных, в том числе и скрытых данных, утечки данных; **Владеет** навыками применения современных способов выявления скрытой цифровой информации.

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

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

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

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

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

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 6 семестре (на 3 курсе) (очная форма обучения).

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Основные понятия и принципы информационной и цифровой безопасности	22	6		6	10
2.	Безопасность устройств и приложений	10	2		6	2
3.	Организация многоуровневой защиты данных	14	6		2	6
4.	Современное программное обеспечение для защиты от несанкционированного воздействия на цифровую информацию	16,8	2		4	7,8
	ИТОГО по разделам дисциплины	59,8	16		18	25,8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	8				
	Общая трудоемкость по дисциплине	74				

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

2.3

2.4 Содержание разделов (тем) дисциплины

2.4.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1.	Основные понятия и принципы информационной и цифровой безопасности	Основы информационной безопасности в РФ. Нормативно-правовые акты, связанные с защитой информации. Формирование цифрового портрета пользователя: угрозы и риски.	Опрос
2.	Безопасность устройств и приложений	Основные варианты уязвимых точек в системах защиты информации, способы обнаружения и упреждения угроз цифровой безопасности	Опрос
3.	Организация многоуровневой защиты данных	Принципы построения многоуровневых систем защиты данных. Базовые понятия о защите вычислительной сети от угроз и различных атак на защиту, данные и целостность работы сети	Опрос
4.	Современное программное обеспечение для защиты от несанкционированного воздействия на цифровую информацию	Безопасность объектов критической информационной инфраструктуры. Обнаружение несанкционированного доступа к информации, передачи скрытой/зашифрованной информации с использованием современных программных продуктов	Опрос

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

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
1.	Основные понятия и принципы информационной и цифровой безопасности	Основные стандарты и принципы информационной безопасности, основные понятия цифровой безопасности; правовые основы информационной безопасности.	ЛР
2.	Безопасность устройств и приложений	Обнаружение угроз стабильной работы в сети, разбор практических ситуаций	Р
3.	Организация многоуровневой защиты данных	Изучение стандартов информационной безопасности и их применимость в различных отраслях и на различных уровнях, включая аппаратный и программный	Опрос
4.	Современное программное обеспечение для защиты от несанкционированного воздействия на цифровую информацию	Защита цифровой информации, гигиена цифрового портрета пользователя, защита электронной почты, персональные данные в сети, угрозы в социальных сетях. Выявление скрытых каналов внедрения в информационный трафик и передачи данных	Р

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

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

2.4.3 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Проработка учебного (теоретического) материала	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 9 от 12.04.2019 г.
2	Выполнение домашних заданий (решение задач)	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 9 от 12.04.2019 г.
3	Подготовка к текущему контролю	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 9 от 12.04.2019 г.
4	Промежуточная аттестация (зачет)	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 9 от 12.04.2019 г.

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

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

– в форме аудиофайла,

– в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

– в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии, применяемые при освоении дисциплины (модуля)

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

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

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

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

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

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

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

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
	ОПК-5.1. Алгоритмизирует задачи на основе существующих методов и стандартных решений при разработке компьютерных программ	**Знает** основные стандарты и принципы информационной безопасности, понятия цифровой безопасности; **Умеет** распознавать угрозы стабильной работы в сети**,** планировать многоуровневую защиту данных, применять методы анализа для выявления уязвимых позиций в программном и аппаратном обеспечении электронно-вычислительных устройств; **Владеет** навыками работы по обнаружению и защите от атак различного вида на цифровую информацию с использованием современного программного обеспечения	Вопрос для устного опроса 1-6, 12-15	Вопрос на зачет 1-11, 19-24
	ОПК-5.2. Реализует алгоритмы с использованием современных средств разработки прикладного программного обеспечения	**Знает** основы криптографической защиты информации, принципы стеганографии и классические алгоритмы шифрования, расшифрования и признаки дешифрования; **Умеет** анализировать цифровые данные и распознавать наличие потока зашифрованных, в том числе и скрытых данных, утечки данных; **Владеет**навыками применения современных способов выявления скрытой цифровой информации.	Вопрос для устного опроса 7-11, 16-18	Вопрос на зачет 12-18, 25-30

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

Примерный перечень вопросов и заданий

Вопросы для устного опроса

1. Основные принципы информационной безопасности.
2. Цифровая безопасность и ее основные отличия. Понятие и формирование цифрового портрета пользователя.
3. Правовые основы защиты информации, персональных данных, и их регулирование.
4. Источники и содержание угроз в информационной сфере.
5. Аппаратное обеспечение безопасности информации.
6. Планирование безопасной работы на персональном компьютере и принципы цифровой гигиены.
7. Организация многоуровневой сетевой защиты данных.
8. Основы криптографической защиты информации. Шифрование с закрытым и открытым ключом.
9. Основы криптографической защиты информации. Шифр Вижинера.

10. Стеганографические методы несанкционированного внедрения в цифровую информацию и их обнаружение.
11. Антивирусная защита и обзор основных качеств современного программного обеспечения в области противовирусной защиты цифровых данных.
12. DDOS-атаки.
13. Основные методы защиты цифровой информации.
14. Определение потенциально возможных точек угроз и нарушителей защиты информации.
15. Брандмауэры и их характеристики.
16. Аппаратные и программные средства защиты информации.
17. Регламентирование и управление доступом к данным.
18. Защита электронной почты. Многофакторная авторизация и аутентификация.

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

1. Основные принципы информационной безопасности.
2. Цифровая безопасность и ее основные отличия. Понятие цифрового портрета пользователя.
3. Правовые основы защиты информации, персональных данных, и их регулирование.
4. Источники и содержание угроз в информационной сфере.
5. Аппаратное обеспечение безопасности информации. Радиоэлектронная борьба.
6. Аппаратное обеспечение безопасности информации. Воздействие на сети.
7. Обеспечение информационной и цифровой безопасности в организации.
8. Характеристика эффективных стандартов по безопасности в РФ.
9. Планирование безопасной работы на персональном компьютере и принципы цифровой гигиены.
10. Организация многоуровневой сетевой защиты данных.
11. Правовые основы сертификации и аттестации средств защиты информации.
12. Основы криптографической защиты информации. Шифрование с закрытым ключом.
13. Основы криптографической защиты информации. Шифрование с открытым ключом.
14. Основы криптографической защиты информации. Симметричные и несимметричные алгоритмы шифрования.
15. Основы криптографической защиты информации. Шифр Вижинера.
16. Стеганографические методы несанкционированного внедрения в цифровую информацию и их обнаружение.
17. Примеры стеганографических систем.
18. Компьютерные вирусы. Стелс-вирусы, трояны, классификация вирусных и вредоносных программ.
19. Антивирусная защита и обзор основных качеств современного программного обеспечения в области противовирусной защиты цифровых данных.
20. Формы атак на информацию. DDOS-атаки.
21. Общие принципы построения защищенного программного обеспечения.
22. Основные методы защиты цифровой информации.
23. Управление безопасностью в защищенных операционных системах.
24. Определение потенциально возможных точек угроз и нарушителей защиты информации.
25. Брандмауэры и их характеристики.
26. Аппаратные и программные средства защиты информации.
27. Регламентирование и управление доступом к данным.
28. Защита электронной почты.
29. Защита IP сетей.
30. Оперативно-диспетчерское управление защитой информации в организации.

Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент в полном объёме демонстрирует знания, умения и навыки в соответствии с ОПК; владеет теоретическими знаниями и практическими умениями по выделенным основным модулям дисциплины.

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

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

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

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

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

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

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Учебная литература

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

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

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

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

5) Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва :Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021.— 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Электронно-

библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/101992.html

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

Электронно-библиотечные системы (ЭБС):

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

Профессиональные базы данных:

1. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/

Информационные справочные системы:

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

Ресурсы свободного доступа:

1. КиберЛенинка (http://cyberleninka.ru/);
2. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
3. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
4. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

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

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

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

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

6. Материально-техническое обеспечение по дисциплине (модулю)

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

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

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