МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.15
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы управления информационной безопасностью
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость:4 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	**5**	**Итого**
Форма контроля / **Вид занятий**	**зачет**	
Лекции	16	16
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.25	0.25
Контактная работа	48.25	48.25
Самостоятельная работа	95.75	95.75
Контроль		
Итого	**144**	**144**

Рабочую программу составил(и):

Власов Игорь Анатольевич

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☒ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Целью освоения дисциплины является – изучение основных понятий, методологии и практических приемов управления технической и организационно инфраструктурой обеспечения информационной безопасности в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ).

Основные задачи изучения дисциплины:

-формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;

-ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем, обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации;

- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, организации и разграничения полномочий персонала, ответственного за информационную безопасность.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Организационно-правовое обеспечение информационной безопасности;
- Международные и российские нормативные акты, и стандарты по информационной безопасности.

Полученные знания используются при изучении следующих дисциплин:

- Техническая защита информации;
- Моделирование процессов и систем защиты информации.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-8 Использует знания современных подходов к управлению ИБ и направления их развития, основных стандартов, регламентирующие управление ИБ	ПК-8.1 Использует знания современных подходы к управлению ИБ и направления их развития, основных стандартов, регламентирующие управление ИБ	Знать: - современные подходы к управлению ИБ и направления их развития; - основные стандарты, регламентирующие управление ИБ; - принципы построения СУИБ; принципы разработки процессов управления ИБ; - взаимосвязи отдельных процессов управления ИБ в

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		рамках общей СУИБ; - подходы к интеграции СУИБ в общую систему управления предприятием
		Уметь: - - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; - применять процессный подход к управлению ИБ в различных сферах деятельности; - используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
		Владеть: -навыками управления информационной безопасностью простых объектов; - навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
	ПК-8.2 Использует знания принципов построения СУИБ и разработки процессов управления ИБ	Знать: - теорию разработки документации по ИБ
		Уметь: -анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; - разрабатывать и внедрять СУИБ и оценивать ее эффективность.
		Владеть: - терминологией и

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		процессным подходом построения систем управления ИБ
	ПК-8.3 Умеет анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ, определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ	Знать: - правила оформления документации по ИБ
		Уметь: - практически решать задачи формализации разрабатываемых процессов управления ИБ;
		Владеть: - навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.
	ПК-8.4 Владеет навыками управления информационной безопасностью простых объектов, терминологией и процессным подходом построения систем управления ИБ	Знать: - процессный подход с СМИБ
		Уметь: - реализовать процессный подход в СМИБ
		Владеть: - навыками построения процессов СМИБ
	ПК-8.5 Демонстрирует навыки построения как отдельных процессов управления ИБ, так и системы процессов в целом	Знать: - методику управления угрозами безопасности информации
		Уметь: - формулировать угрозы и риски
		Владеть: - навыками определения угроз безопасности
ПК-9 Способен формулировать политики информационной безопасности	ПК-9.4 Использует знания федерального законодательства, других руководящих документов при разработке ОРД	Знать: - современные подходы к управлению ИБ и направления их развития; - основные стандарты, регламентирующие управление ИБ; - принципы построения СУИБ; принципы разработки процессов управления ИБ; - взаимосвязи отдельных процессов управления ИБ в

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		рамках общей СУИБ; - подходы к интеграции СУИБ в общую систему управления предприятием Уметь: - - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; - применять процессный подход к управлению ИБ в различных сферах деятельности; - используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; Владеть: -навыками управления информационной безопасностью простых объектов; - навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
	ПК-9.5 Умеет разработать Политику информационной безопасности	Знать: - теорию разработки документации по ИБ Уметь: -анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; - разрабатывать и внедрять СУИБ и оценивать ее эффективность. Владеть: - терминологией и процессным подходом

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		построения систем управления ИБ
	ПК-9.6 Владеет стилистикой оформления документации	Знать: - правила оформления документации по ИБ Уметь: - практически решать задачи формализации разрабатываемых процессов управления ИБ; Владеть: - навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Основные понятия управления информационной безопасностью Понятие информационной безопасности. Основные составляющие информационной безопасности. Управление информационной безопасностью. Стандарты СМИБ. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Критерии эффективности СУИБ. Структура и шкала ценности информации. Определение границ системы управления ИБ. Система менеджмента ЗИ. Координация обеспечения ИБ. Положения и принципы СУИБ.	5	2		-	Вопросы к зачету
Модуль 1	Пр	Тема 1 1 Основные понятия управления информационной безопасностью Определение границ системы управления информационной	5	4			Отчет по практическому занятию №1

		безопасностью и конкретизация целей ее создания.					
Модуль 1	Ср	Тема 1 1 Основные понятия управления информационной безопасностью Самостоятельное изучение материала, не вошедшего в курс лекций	5	12			Вопросы к зачету
Модуль 1	Лек	Тема 2 Процессорный подход в управлении ИБ Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ).. Аудит ИБ. Оценка соответствия мер защиты требованиям ИБ.	5	2		-	Вопросы к зачету
Модуль 1	Пр	Тема 2 Процессорный подход в управлении ИБ Аудит безопасности в соответствии с ГОСТ Р ИСО/МЭК 27001.		4			Отчет по практическому занятию №2
Модуль 1	Ср	Тема 2 Процессорный подход в управлении ИБ Самостоятельное изучение материала, не вошедшего в	5	12			Вопросы к зачету

		курс лекций					
Модуль 1	Лек	Тема 3 Основные процессы СУИБ. Создание СУИБ в организации. Определение целей и задач СУИБ. Процесс «Мониторинг эффективности» Процессы «Управление документами». Процесс «Ответственность руководства». Процесс «Подготовка, осведомленность и квалификация персонала». Процессы «Анализ угроз и рисков». (включая разработку метрик эффективности). Понятие «Зрелость процесса». Политика ИБ. «Анализ со стороны высшего руководства». Принципы СУИБ. Процесс выстраивания культуры ИБ. Недопустимые события. Этапы внедрения. COBIT5.	5	2			Вопросы к зачету
Модуль 1	Пр	Тема 3 Основные процессы СУИБ. Создание СУИБ в организации Практическая разработка процессов СУИБ. Расчет метрик		4			Отчет по практическому занятию №3

		информационной безопасности.					
Модуль 1	Ср	Тема 3 Основные процессы СУИБ. Создание СУИБ в организации Самостоятельное изучение материала, не вошедшего в курс лекций	5	12			Вопросы к зачету
Модуль 1	Лек	Тема 4 Современные методы и средства анализа и управление рисками информационных систем. Тренды и проблемы управления рисками. Структура информационного риска. Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Метод оценки рисков на основе модели угроз и уязвимостей.	5	2		-	Вопросы к зачету
Модуль 1	Пр	Тема 4 Современные методы и средства анализа и управление рисками информационных систем Технологии (методики) управления	5	4			Отчет по практическому занятию №4

		информационными рисками					
Модуль 1	Ср	Тема 4 Современные методы и средства анализа и управление рисками информационных систем Самостоятельное изучение материала, не вошедшего в курс лекций	5	12			Вопросы к зачету
Модуль 1	Лек	Тема 5 Эффективное построение ИБ, оценка зрелости процессов ИБ. Методика оценки зрелости процессов ИБ. Домены и направления процессов ИБ. План развития ИБ. Управление инцидентами ИБ.	5	2			Вопросы к зачету
Модуль 1	Пр	Тема 5 Эффективное построение ИБ, оценка зрелости процессов ИБ. Оценка рисков	5	4			Отчет по практическому занятию №5
Модуль 1	Ср	Тема 5 Эффективное построение ИБ, оценка зрелости процессов ИБ. Самостоятельное изучение материала, не вошедшего в курс лекций	5	12			Вопросы к зачету
Модуль 1	Лек	Тема 6 Управление угрозами безопасности информации. БДУ ФСТЭК.. Тактики и техники.. Сравнение тактик и техник. Виды и классификация угроз. Нарушители.	5	2			Вопросы к зачету

		Уязвимости. Управление уязвимостями.					
Модуль 1	Пр	Тема 6 Управление угрозами безопасности информации. Выявление угроз информационной безопасности	5	4			Отчет по практическому занятию №6
Модуль 1	Ср	Тема 6 Управление угрозами безопасности информации. Самостоятельное изучение материала, не вошедшего в курс лекций	5	12			Вопросы к зачету
Модуль 1	Лек	Тема 7 Экономика защиты информации Система ресурсообеспечения защиты информации и эффективность еѐ использования	5	2			Вопросы к зачету
Модуль 1	Пр	Тема 7 Экономика защиты информации Прогнозирование и планирование затрат на ИБ	5	4			Отчет по практическому занятию №7
Модуль 1	Ср	Тема Экономика защиты информации Самостоятельное изучение материала, не вошедшего в курс лекций	5	11			Вопросы к зачету
Модуль 1	Лек	Тема 8 Некоторые аспекты практической СУИБ. План DRP. Управление персоналом и ИБ. Кадровые решения в	5	2			Вопросы к зачету

		организации по информационной безопасности. Безопасность, связанная с персоналом Обеспечение ИБ при малом бюджете. Практические вопросы. План DRP					
Модуль 1	Пр	Тема 8 Некоторые аспекты практической СУИБ. План DRP. Разработка верхнеуровневых документов по ИБ.	5	4			Отчет по практическому занятию №8
Модуль 1	Ср	Тема 8 Некоторые аспекты практической СУИБ. План DRP. Самостоятельное изучение материала, не вошедшего в курс лекций	5	12.75			Вопросы к зачету
	ПА	Сдача зачета (итоговый тест/сдача зачета устно (письменно)	5	0,25		-	Банк тестовых заданий /Вопросы к зачету
			Итого:	**144**			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. **CD-технология** – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
5	ПК-9, ПК-8	Протоколы практических заданий №1-8
		Вопросы к зачету №№1-45

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Определение границ системы управления информационной безопасностью и конкретизация целей ее создания.
2	Аудит безопасности в соответствии с ГОСТ Р ИСО/МЭК 27001.
3	Практическая разработка процессов СУИБ. Расчет метрик информационной безопасности.
4	Технологии (методики) управления информационными рисками
5	Оценка рисков
6	Выявление угроз информационной безопасности
7	Прогнозирование и планирование затрат на ИБ
8	Разработка верхнеуровневых документов по ИБ

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты изучают ОРД и ГОСТы по управлению ИБ, согласно выбранных вариантов заданий разрабатывают процессы СУИБ, определяют границы СУИБ, рассчитывают метрики и разрабатывают плейбуки и план восстановления после аварийных ситуаций на инфраструктуре предприятия.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.

- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.2.2. Типовой пример тестового задания

Последовательность действий работника в случае выявления инцидента ИБ:

Выберите один или несколько вариантов ответа:
1) прекратить работу с ресурсом, в котором выявлен инцидент ИБ
2) оповестить непосредственного руководителя о факте выявления инцидента ИБ
3) заблокировать ресурс
4) приступить к ликвидации последствий инцидента

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 5

№ п/п	Вопросы к зачету
1.	Сущность и функции управления ИБ.
2.	Принципы, подходы и виды управления.
3.	Цели и задачи управления ИБ.
4.	Понятие системы управления.
5.	Методы и средства управления безопасностью информации и защитой информации.
6.	Комплекс методов и средств защиты информации как объект управления ИБ
7.	Процесс ITIL: Управление информационной безопасностью.
8.	Процессный подход к управлению информационной безопасностью
9.	Суть процессного подхода.
10.	Классификация и атрибуты процессов.
11.	Процессы управления и обеспечения информационной безопасности.
12.	Ключевые процессы СУИБ.
13.	ISO/IEC 27001 и система управления информационной безопасности
14.	Механизм взаимодействия и применения стандартов системы управления ИБ
15.	Существующие стандарты и методологии по управлению ИБ.
16.	Способы оценки информационной безопасности. Метрики информационной безопасности (ISO 27004, NIST 800-55).
17.	Система управление рисками по требованию стандарта ISO 27001:2005.
18.	Цель процесса анализа рисков ИБ.

19.	Этапы и участники процесса анализа рисков ИБ.
20.	Построение системы контроля рисков, процедур, средств управления ИБ.
21.	Алгоритм определения рисков.
22.	Идентификация и оценка активов.
23.	Идентификация уязвимостей.
24.	Реестр рисков.
25.	Управление рисками.
26.	Инциденты ИБ и законодательство РФ.
27.	Процесс управления инцидентами ИБ.
28.	Реагирование на инцидент ИБ.
29.	Общий алгоритм действий при наступлении инцидента.
30.	Схема процессов управления инцидентами
31.	Взаимодействие с НКЦКИ и ГосСопка по компьютерным инцидентам
32.	Определение целей управления информационной безопасностью.
33.	Политика ИБ
34.	Структура политики информационной безопасности и процесс ее разработки.
35.	Проведение предварительного исследования состояния информационной безопасности.
36.	Разработка политики безопасности.
37.	Внедрение разработанных политик безопасности.
38.	Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию (цикл)
39.	Проверка соответствия политике безопасности и реализация Планов по ИБ
40.	Служба защиты информации, ее назначение. Место службы защиты информациив системе безопасности
41.	Организационные задачи и функции службы защиты информации.
42.	Задачи, функции, права и ответственность руководителя и руководителей под-разделений службы защиты информации.
43.	Персонал предприятия как объект защиты.
44.	Cobit5, особенности управления ИБ по зарубежным стандартам
45.	DRP

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
5	Зачет (письменно/по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Нестеров С.А.	Основы информационной безопасности	учебное пособие	2022	
2	Прохорова О. В.	Информационная безопасность и защита информации	учебное пособие	2022	
3	И.С. Поздняк, И.С. Макаров, Л.Р. Чупахина	Планирование и управление информационной безопасностью	учебное пособие	2020	

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Ясенев В.Н.	Информационная безопасность	учебное пособие	2019	
2	Е.В. Вострецова	Основы информационной безопасности	учебное пособие	2019	

8.3. Перечень профессиональных баз данных и информационных справочных систем

Интернет-портал для ИТ-специалистов - http://www.habrahabr.ru/
Интернет-портал ресурсов по информационной безопасности - http//www.all-ib.ru
Консультант Плюс - http://www.consultant.ru/
Официальный портал правовой информации - http://pravo.gov.ru/
Официальный сайт Федеральной службы по техническому и экспортному контролю - http://www.fstec.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	УЛК -310	
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф