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

Б1.В.ДВ.04.01
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение безопасности критической информационной инфраструктуры
(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: 5 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	**8**	**Итого**
Форма контроля / **Вид занятий**	**зачет**	
Лекции	12	12
Лабораторные	-	-
Практические	48	48
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.25	0.25
Контактная работа	60,25	60,25
Самостоятельная работа	119.75	119.75
Контроль	-	-
Итого	**180**	**180**

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

Цель освоения дисциплины являчется изучение основных понятий, методологии и практических приемов обеспечения безопасности объектов критической информационной инфраструктуры.

Задачи изучения дисциплины:

1) изучение основных понятий и технологий обеспечения информационной безопасности объектов критической информационной инфраструктуры;

2) получение знаний и навыков защиты объектов критической информационной инфраструктуры;

3) изучение нормативно-правовых актов, регулирующих вопросы создания, эксплуатации и защиты объектов критической информационной инфраструктуры;

4) приобретение обучаемыми необходимого объема знаний в области организации работы по защите объектов критической информационной инфраструктуры;

5) формирование у обучаемых целостного представления о внедрении системного подхода к решению задач обеспечения информационной безопасности

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Организационно-правовые нормы обеспечения информационной безопасности.

Знания и практические навыки, полученные при изучении дисциплины «Безопасность объектов критической информационной инфраструктуры», используются при написании выпускной квалификационной работы.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-10 Способен осуществлять моделирование решений по реализации программного обеспечения и управлению БД	ПК-10.12 Владеет алгоритмами создания системы комплексной защиты, методологией разработки моделей	Знает: - алгоритм создания системы комплексной защиты, методологию разработки моделей Умеет: - разрабатывать ролевую матрицу доступа Владеет: - инструментарием имитационного моделирования

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-11 Способен противодействовать угрозам безопасности информации с использованием средств защиты информации операционных систем и сетей, включая средства криптографической защиты информации	ПК-11.13 Использует знания нормативно-правовых актов и методических документов по защите информации, угрозы безопасности информации КИИ	Знать: - виды конфиденциальной информации, нормативно-правовые акты и методические документы по защите информации, угрозы безопасности информации Уметь: - разрабатывать технические задания на создание системы обеспечения информационной безопасности Владеть: - навыками формирования требований к системе обеспечения информационной безопасности
	ПК-11.14 Умеет определять актуальные угрозы безопасности критической информационной инфраструктуры	Знать: - типы актуальных угроз КИИ
		Уметь: - выявить критические процессы и активы субъекта КИИ - определять актуальные угрозы безопасности информации
		Владеть: - приемами обеспечения безопасности объектов критической информационной инфраструктуры
	ПК-11.15 Владеет навыками формирования требований к системе обеспечения безопасности КИИ	Знать: - требования к обеспечению безопасности КИИ
		Уметь: - организовать и провести категорирование ОКИИ
		Владеть: -навыками проведения классификации информационных систем по требованиям защиты информации

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 Субъекты КИИ: понятие, определение принадлежности 1.ФЗ 187 «О безопасности критической информационной инфраструктуры» 2.Объекты критической информационной инфраструктуры: основные понятия, термины и определения. 3.Права субъектов критической информационной инфраструктуры 4.Обязанности субъектов КИИ 5.Самоопределение принадлежности к КИИ 6. Набор документов для определения является ли организация субъектом КИИ 7. Дорожная карта по выполнению требований Федерального закона «О безопасности критической информационной инфраструктуры» 8. Основные понятия, термины и определения в области обеспечения безопасности ЗОКИИ. Система безопасности ЗОКИИ	8	2		-	Вопросы к зачету
Модуль 1	Пр	Тема 1 Субъекты КИИ: понятие, определение принадлежности Самоопределение субъекта по ФЗ 187	8	4			Отчет по практическому занятию №1
Модуль 1	Пр	Тема 1 Субъекты КИИ: понятие, определение принадлежности Составление Дорожной карты по выполнению требований	8	4			Отчет по практическому занятию №2

		законодательства РФ					
Модуль 1	Пр	Тема 1 Субъекты КИИ: понятие, определение принадлежности Мероприятия по определению оснований для отнесения организации к объектам критической информационной инфраструктуры	8	4			Отчет по практическому занятию №3
Модуль 1	Ср	Тема 1 Субъекты КИИ: понятие, определение принадлежности	8	20			Вопросы к зачету
Модуль 1	Лек	Тема 2 Объекты КИИ: типы и виды 1.Типы объектов КИИ 2.Классификазия ОКИИ по значимости 3.Реестр значимых объектов КИИ 4. Классификазия ОКИИ по видам систем 5. Основные нормативно-правовые акты, устанавливающие меры защиты объекта КИИ	8	2		-	
Модуль 1	Пр	Тема 2 Объекты КИИ: типы и виды Оценка объектов КИИ субъекта КИИ	8	4			Отчет по практическому занятию №4
Модуль 1	Ср	Тема 2 Объекты КИИ: типы и виды	8	20			Вопросы к зачету
Модуль 1	Лек	Тема 3. Категорирование объектов КИИ 1. Правила категорирования объектов критической информационной инфраструктуры 2. Формирование комиссии по категорированию 3. Подготовка перечня объектов КИИ подлежащих категорированию 4. Категорирование (присвоение объекту КИИ категории, либо принятие мотивированного решения об отсутствии необходимости в ее присвоении) 5. Оценка объектов КИИ в	8	2			Вопросы к зачету

		соответствии с показателями критериев значимости 6. Подготовка итоговых документов по результатам категорирования 7. Сроки категорирования 8. Реестр значимых объектов КИИ. Цель ведения реестра					
Модуль 1	Пр	Тема 3. Категорирование объектов КИИ Проведение инвентаризации объектов КИИ	8	4			Отчет по практическому занятию №5
Модуль 1	Пр	Тема 3. Категорирование объектов КИИ Категорирование объектов КИИ	8	4			Отчет по практическому занятию №6
Модуль 1 Тема 3.	Ср	Категорирование объектов КИИ	8	20			Вопросы к зачету
Модуль 1	Лек	Тема 4 Обеспечение безопасности значимых объектов кии 1. Этапы создания и функционирования СОИБ ЗОКИИ 2. Аудит информационной безопасности ЗОКИИ 3.Моделирование угроз ЗООКИИ 4. Уровень зрелости процессов информационной безопасности по методологии ISF 5. План мероприятий по обеспечению безопасности ЗОКИИ 6. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия 7. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа потенциальных уязвимостей ЗОКИИ, возможных способов	8	2			Вопросы к зачету

		реализации (возникновения) угроз безопасности информации и последствий от их реализации					
Модуль 1	Пр	Тема 4 Обеспечение безопасности значимых объектов кии Составление модели угрорз ЗОКИИ	8	4			Отчет по практическому занятию №7
Модуль 1	Пр	Тема 4 Обеспечение безопасности значимых объектов кии План мероприятий по обеспечению безопасности ЗОКИИ	8	4			Отчет по практическому занятию №8
Модуль 1	Ср	Тема 4 Обеспечение безопасности значимых объектов кии	8	20			Вопросы к зачету
Модуль 1	Лек	Тема 5 Организационные и технические меры по обеспечению безопасности ЗОКИИ 1 Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «тТребования по обеспечению безопасности ЗОКИИ» 2. Технологии обеспечения безопасности критической информационной инфраструктуры 3. Принципы обеспечения безопасности критической информационной инфраструктуры 4. Состав и содержание организационных и технических мер по обеспечению безопасности ЗОКИИ	8	2		-	Вопросы к зачету
Модуль 1	Пр	Тема 5 Организационные и технические меры по обеспечению безопасности ЗОКИИ Организационные и технические меры по обеспечению безопасности ЗОКИИ	8	4			Отчет по практическому занятию №9
Модуль 1	Ср	Тема 5 Организационные и технические меры по обеспечению безопасности ЗОКИИ	8	20			Вопросы к зачету
Модуль 1	Лек	Тема 6 Взаимодействие с	8	2			Отчет по

		ГОССОПКА. Практические вопросы взаимодействия с регуляторами 1.НПА по порядку взаимодействия с ГОССОПКА 2.Назначение и функции ГОССОПКА, НКЦКИ 3.Структура ГОССОПКА 4. Методы организации взаимодействия 5. Содержание мероприятий 6. Комплект документации					практическому занятию №10
Модуль 1	Пр	Тема 6 Взаимодействие с ГОССОПКА. Практические вопросы взаимодействия с регуляторами Разработка схемы взаимодействия с ГосСОПКА	8	4			Вопросы к зачету
Модуль 1	Пр	Тема 6 Взаимодействие с ГОССОПКА. Практические вопросы взаимодействия с регуляторами Расчет показателей категории значимости ЗООКИИ	8	4			Отчет по практическому занятию №11
Модуль 1	Пр	Тема 6 Взаимодействие с ГОССОПКА. Практические вопросы взаимодействия с регуляторами Методика проектирования и построения схемы защиты объектов КИИ	8	4			Отчет по практическому занятию №12
Модуль 1	Ср	Тема 6 Взаимодействие с ГОССОПКА. Практические вопросы взаимодействия с регуляторами	8	19.75			Вопросы к зачету
	ПА	Сдача зачета (итоговый тест/сдача зачета устно (письменно)	8	0,25		-	Банк тестовых заданий /Вопросы к зачету
			Итого:	**180**			

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
8	ПК-11, ПК-10	Протоколы практических заданий №1-12
		Вопросы к зачету №№1-45
		Темы для реферата

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

7.2.1

- Реферат «Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры»
- Реферат «Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»

7.2.2. Самостоятельная работа

Ознакомиться с нормативными актами по обеспечению безопасности объектов критической информационной инфраструктуры:

−Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

−Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

−Постановление Правительства РФ от 13.04.2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»;

−Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

−Информационное сообщение ФСТЭК России по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий от 24 августа 2018 г. № 240/25/3752;

−Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.;

−Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры;

−Информационное сообщение ФСТЭК России о методических документах по вопросам обеспечения безопасности информации в ключевых системах

информационной инфраструктуры Российской Федерации от 4 мая 2018 г. № 240/22/2339.

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Самоопределение субъекта по ФЗ 187
2	Составление Дорожной карты по выполнению требований законодательства РФ
3	Мероприятия по определению оснований для отнесения организации к субъекту КИИ
4	Оценка объектов КИИ субъекта КИИ
5	Проведение инвентаризации объектов КИИ
6	Категорирование объектов КИИ
7	Составление модели угрорз ЗОКИИ
8	План мероприятий по обеспечению безопасности ЗОКИИ
9	Организационные и технические меры по обеспечению безопасности ЗОКИИ
10	Разработка схемы взаимодействия с ГосСОПКА
11	Расчет показателей категории значимости ЗООКИИ
12	Методика проектирования и построения схемы защиты объектов КИИ

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты изучают и практически отрабатывают требования ФЗ 187 «О критической информационной инфраструктуре», для выбранного варианта организации проводят инвентаризацию. объектов КИИ, проводят категорирование объектов КИИ, составляют модель угроз, разрабатывают Организационные и технические меры по обеспечению безопасности ЗОКИИ.

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.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 8

№ п/п	Вопросы к зачету
1.	1. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры
2.	Принципы обеспечения безопасности критической информационной инфраструктуры
3.	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
4.	Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры
5.	Категорирование объектов критической информационной инфраструктуры
6.	Реестр значимых объектов критической информационной инфраструктуры
7.	Права и обязанности субъектов критической информационной инфраструктуры
8.	Система безопасности значимого объекта критической информационной инфраструктуры
9.	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
10.	Оценка безопасности критической информационной инфраструктуры
11.	Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры
12.	Ответственность за нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов
13.	Регламентация правил и процедур аудита безопасности
14.	Перечень показателей критериев ЗОКИИ и их значения
15.	Оценка в соответствии с перечнем показателей критериев ЗОКИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ
16.	Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности ЗОКИИ
17.	Основные нормативно-правовые акты, устанавливающие меры защиты объекта КИИ
18.	Правила категорирования объектов критической информационной инфраструктуры
19.	Каковы этапы создания и функционирования СОИБ ЗОКИИ
20.	Технологии обеспечения безопасности критической информационной инфраструктуры

21.	Принципы обеспечения безопасности критической информационной инфраструктуры
22.	Состав плана мероприятий по СИБ ЗООКИИ
23.	Алгоритм категорирования вновь создаваемых ОКИИ
24.	Порядок изменений в Перечне ОКИИ, подлежащих категорированию
25.	Порядок информирования НКЦКИ об компьютерных инцидентах
26.	Схема взаимодействия с ГОССОПКА
27.	Порядок Перевода не значимого ОКИИ в ЗОКИИ
28.	Порядок исключения ИС/АСУ/ИТКС из объектов КИИ
29.	Порядок реагирования на компьютерные инциденты с ЗОКИИ
30.	Методы организации взаимодействия с ГОССОПКА
31.	Перечень информации, передаваемой в ГосСОПКА
32.	Что делать с объектами КИИ не имеющими категорию значимости: как их учитывать, как это фиксировать, оформлять и т.п.?
33	Порядок обработки замечаний от ФСТЭК (после отправки Перечня объектов КИИ и после отправки сведений об объектах КИИ)
34	С кем нужно согласовывать Перечень объектов КИИ, подлежащих категорированию?
35	Алгоритм перевода ЗОКИИ в незначимые ОКИИ
36	Требования к специалисту безопасности ЗОКИИ
37	Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ
38	Виды контроля (мониторинга) за обеспечением уровня безопасности значимого объекта КИИ и его системы безопасности
39	Мониторинг событий безопасности и контроль за действиями персонала в значимом объекте КИИ
40	Порядок документирования процедур и результатов контроля за обеспечением уровня безопасности значимого объекта КИИ
41	Реагирование на компьютерные инциденты в ходе эксплуатации ЗОКИИ
42	Требования к классам защиты средств защиты информации и средствам вычислительной техники для различных категорий значимости объектов КИИ
43	Требования к силам обеспечения безопасности значимых объектов КИИ
44	Структура системы безопасности ЗОКИИ
45	Этапы жизненного цикла системы безопасности ЗОКИИ

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
8	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	Ерохин С.Д.	Управление безопасностью критических информационных инфраструктур	Научное издание	2021	
2	А.П. Курило	Основы управления информационной безопасностью [Электронный ресурс]	учебное пособие	2021	http://www.iprbookshop.ru/12021

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	Милославская Н.Г.	Проверка и оценка деятельности по управлению информационной безопасностью [Электронный ресурс]	учебное пособие	2021	http://www.iprbookshop.ru/12032.— ЭБС «IPRbooks»

8.3. Перечень профессиональных баз данных и информационных справочных систем

1. «КонсультантПлюс» - компьютерная справочно-правовая система по законодательству России – http://www.consultant.ru/
2. Информационная система «Единое окно доступа к информационным ресурсам». - http://window.edu.ru/
3. ФСТЭК России (Федеральная служба по техническому и экспортному контролю) Адрес ресурса: https://fstec.ru
4. CNEWS безопасность Адрес ресурса: https://safe.cnews.ru/

9. 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	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
	аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. 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