МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА"

СОГЛАСОВАНО
Зав. выпускающей кафедры

УТВЕРЖДАЮ
Проректор по УР

А.В. Корячко

Спецдисциплина 4

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационной безопасности**

Учебный план 10.05.01 _23_00.plx
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Квалификация **специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	16	16	16	16
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	48,25	48,25	48,25	48,25
Контактная работа	48,25	48,25	48,25	48,25
Сам. работа	51	51	51	51
Часы на контроль	8,75	8,75	8,75	8,75
Итого	108	108	108	108

г. Рязань

Программу составил(и):
к.т.н., зав. каф., Пржегорлинский Виктор Николаевич

Рабочая программа дисциплины
Спецдисциплина 4

разработана в соответствии с ФГОС ВО:
ФГОС ВО - специалитет по специальности 10.05.01 Компьютерная безопасность (приказ Минобрнауки России от 26.11.2020 г. № 1459)

составлена на основании учебного плана:
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
утвержденного учёным советом вуза от 28.04.2023 протокол № 11.

Рабочая программа одобрена на заседании кафедры
Информационной безопасности

Протокол от 29.06.2022 г. № 12
Срок действия программы: 2023-2029 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2024 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2025 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры

Информационной безопасности

Протокол от __ _____ 2027 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является освоение обучающимися методов, средств и мер обеспечения информационной безопасности создания, развития и эксплуатации компьютерной системы в защищенном исполнении (КСЗИ).
1.2	Задачами изучения дисциплины являются:
1.3	- развитие у обучающихся системного мышления и обеспечение более глубокого понимания свойств среды создания, развития и эксплуатации КСЗИ и процессов ее создания, развития и эксплуатации;
1.4	- получение обучающимися знаний методов, средств и участников обеспечения информационной безопасности процессов создания, развития и эксплуатации КСЗИ;
1.5	- приобретение практических навыков решения задач обеспечения информационной безопасности создания, развития и эксплуатации автоматизированных систем КСЗИ.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.2	Преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-5.2: Способен осуществлять разработку проектных решений и документации компонентов систем защиты информации компьютерных систем объектов информатизации, а также мероприятий по обеспечению информационной безопасности процесса их создания;

ОПК-5.2.4. Определяет и реализует требования по обеспечению информационной безопасности процесса созданию компьютерных систем объектов информатизации

Знать
объекты обеспечения информационной безопасности процесса создания АСЗИ;
меры и средства обеспечения информационной безопасности процесса создания (развития) КСЗИ ОИ.

Уметь
определять объекты обеспечения информационной безопасности процесса создания КСЗИ ОИ и формировать для них перечни и модели угроз информационной безопасности;
определять требования по обеспечению информационной безопасности процесса создания КСЗИ ОИ, адекватные угрозам информационной безопасности;
определять меры и средства обеспечения информационной безопасности процесса создания КСЗИ ОИ адекватные конкретным угрозам информационной безопасности.

Владеть
навыками поиска и работы с документами в области обеспечения информационной безопасности процесса создания КСЗИ ОИ;
терминологией в области обеспечения информационной безопасности процесса создания КСЗИ ОИ.

ОПК-5.3: Способен организовывать и осуществлять ввод компьютерной системы объекта информатизации в эксплуатацию;

ОПК-5.3.3. Определяет требования по обеспечению информационной безопасности процесса эксплуатации компьютерных систем объектов информатизации

Знать
объекты обеспечения информационной безопасности процесса эксплуатации КСЗИ ОИ;
угрозы информационной безопасности объектам обеспечения информационной безопасности процесса эксплуатации КСЗИ ОИ.

Уметь
определять объекты обеспечения информационной без-опасности процесса эксплуатации КСЗИ ОИ и формировать для них перечни и модели угроз информационной безопасности;
определять требования по обеспечению информационной безопасности процесса эксплуатации КСЗИ ОИ, адекватные угрозам информационной безопасности.

Владеть
терминологией в области обеспечения информационной безопасности эксплуатации КСЗИ ОИ;
Навыками поиска и работы с документами в области обеспечения информационной безопасности эксплуатации КСЗИ ОИ.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	объекты обеспечения информационной безопасности процесса создания АСЗИ;
3.1.2	меры и средства обеспечения информационной безопасности процесса создания (развития) КСЗИ ОИ;
3.1.3	объекты обеспечения информационной безопасности процесса эксплуатации КСЗИ ОИ;
3.1.4	угрозы информационной безопасности объектам обеспечения информационной безопасности процесса эксплуатации КСЗИ ОИ.
3.2	**Уметь:**
3.2.1	определять объекты обеспечения информационной безопасности процесса создания КСЗИ ОИ и формировать для них перечни и модели угроз информационной безопасности;
3.2.2	определять требования по обеспечению информационной безопасности процесса создания КСЗИ ОИ, адекватные угрозам информационной безопасности;
3.2.3	определять меры и средства обеспечения информационной безопасности процесса создания КСЗИ ОИ адекватные конкретным угрозам информационной безопасности;
3.2.4	определять объекты обеспечения информационной без-опасности процесса эксплуатации КСЗИ ОИ и формировать для них перечни и модели угроз информационной безопасности;
3.2.5	определять требования по обеспечению информационной безопасности процесса эксплуатации КСЗИ ОИ, адекватные угрозам информационной безопасности.
3.3	**Владеть:**
3.3.1	навыками поиска и работы с документами в области обеспечения информационной безопасности процесса создания КСЗИ ОИ;
3.3.2	терминологией в области обеспечения информационной безопасности процесса создания КСЗИ ОИ;
3.3.3	терминологией в области обеспечения информационной безопасности эксплуатации КСЗИ ОИ;
3.3.4	Навыками поиска и работы с документами в области обеспечения информационной безопасности эксплуатации КСЗИ ОИ.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1. Введение в дисциплину					
1.1	Введение в дисциплину /Тема/	10	0			
1.2	Цели и задачи изучения, место дисциплины в структуре основной профессиональной образовательной программы подготовки специалиста по защите информации. Планируемые результаты обучения по дисциплине. Виды и объемы учебной работы и содержание дисциплин. Перечень основных объектов и процессов, изучаемых в дисциплине. Основные объекты, изучаемые в дисциплине, их определения и взаимосвязь. Основные процессы, изучаемые в дисциплине, их определения и взаимосвязь. Взаимосвязь основных объектов и процессов, изучаемых в дисциплине. /Лек/	10	4	ОПК-5.3.3-В ОПК-5.3.3-У ОПК-5.3.3-З ОПК-5.2.4-В ОПК-5.2.4-У ОПК-5.2.4-З	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
1.3	Изучение взаимосвязи основных объектов и процессов, изучаемых в дисциплине /Пр/	10	2	ОПК-5.3.3-В ОПК-5.3.3-У ОПК-5.3.3-З ОПК-5.2.4-В ОПК-5.2.4-У ОПК-5.2.4-З	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

1.4	Изучение конспекта лекций. /Ср/	10	4	ОПК-5.3.3-В ОПК-5.3.3-У ОПК-5.3.3-З ОПК-5.2.4-В ОПК-5.2.4-У ОПК-5.2.4-З	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	подготовка конспекта по вопросам темы.
	Раздел 2. Информационная безопасность деятельности.					
2.1	Информационная безопасность деятельности. /Тема/	10	0			
2.2	Деятельность, ее составляющие и их взаимосвязь. Обеспечение информационной безопасности деятельности. Создание КСЗИ как деятельность, ее составляющие и их взаимосвязь. Обеспечение информационной безопасности создания КСЗИ. Обеспечение информационной безопасности эксплуатации КСЗИ. /Лек/	10	4	ОПК-5.3.3-У ОПК-5.3.3-В ОПК-5.3.3-З ОПК-5.2.4-В ОПК-5.2.4-У ОПК-5.2.4-З	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
2.3	Изучение конспекта лекций. /Ср/	10	5	ОПК-5.3.3-У ОПК-5.3.3-В ОПК-5.3.3-З ОПК-5.2.4-В ОПК-5.2.4-У ОПК-5.2.4-З	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	подготовка конспекта по вопросам темы.
	Раздел 3. Объекты и угрозы обеспечения информационной безопасности создания КСЗИ.					
3.1	Объекты и угрозы обеспечения информационной безопасности создания КСЗИ. /Тема/	10	0			
3.2	Объекты обеспечения информационной безопасности создания КСЗИ: объекты обеспечения информационной безопасности на предпроектных стадиях создания КСЗИ; объекты обеспечения информационной безопасности на стадиях проектирования (разработки) КСЗИ; объекты обеспечения информационной безопасности при вводе КСЗИ в действие. Угрозы информационной безопасности создания КСЗИ: угрозы информационной безопасности, реализуемые на предпроектных стадиях создания КСЗИ; угрозы информационной безопасности, реализуемые на стадиях проектирования (разработки) КСЗИ; угрозы информационной безопасности, реализуемые при вводе КСЗИ в действие. /Лек/	10	10	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
3.3	Определение объектов обеспечения информационной безопасности создания КСЗИ на за-данной стадии или заданном этапе ее создания /Пр/	10	4	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

3.4	Определение перечня и модели угроз информационной безопасности объектов информационной безопасности создания КСЗИ на заданной стадии или заданном этапе ее создания, оценка полноты перечня /Пр/	10	4	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
3.5	Изучение конспекта лекций. /Ср/	10	17	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	подготовка конспекта по вопросам темы.
	Раздел 4. Меры и участники работ по обеспечению информационной безопасности создания КСЗИ.					
4.1	Меры и участники работ по обеспечению информационной безопасности создания КСЗИ. /Тема/	10	0			
4.2	Меры обеспечения информационной безопасности создания КСЗИ: меры обеспечения информационной безопасности, реализуемые на предпроектных стадиях создания КСЗИ; меры обеспечения информационной безопасности, реализуемые на стадиях проектирования (разработки) КСЗИ; меры обеспечения информационной безопасности, реализуемые при вводе КСЗИ в эксплуатацию. Участники работ по обеспечению информационной безопасности создания КСЗИ: участники работ по обеспечению информационной безопасности на предпроектных стадиях создания КСЗИ; участники работ по обеспечению информационной безопасности на стадиях проектирования (разработки) КСЗИ; участники работ по обеспечению информационной безопасности при вводе КСЗИ в действие. /Лек/	10	8	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
4.3	Определение мер обеспечения информационной безопасности объектов обеспечения информационной безопасности создания КСЗИ на заданной стадии или заданном этапе ее создания, адекватных актуальных угрозам их информационной безопасности. /Пр/	10	4	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.
4.4	Оценка качества (полноты, непротиворечивости, эффективности) определенных мер обеспечения информационной безопасности объектов обеспечения информационной безопасности создания КСЗИ. /Пр/	10	2	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Устный опрос по теме. Решение задач. Проверка домашнего задания.

4.5	Изучение конспекта лекций. /Ср/	10	17	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	подготовка конспекта по вопросам темы.
	Раздел 5. Обеспечение информационной безопасности эксплуатации КСЗИ.					
5.1	Обеспечение информационной безопасности эксплуатации КСЗИ. /Тема/	10	0			
5.2	Объекты обеспечения информационной безопасности эксплуатации КСЗИ. Угрозы информационной безопасности эксплуатации КСЗИ. Меры обеспечения информационной безопасности эксплуатации КСЗИ. Участники работ по обеспечению информационной безопасности КСЗИ. /Лек/	10	4	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.
5.3	Изучение конспекта лекций. /Ср/	10	6	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	подготовка конспекта по вопросам темы.
	Раздел 6. Особенности обеспечения информационной безопасности создания и эксплуатации КСЗИ, обрабатывающей информацию, содержащую сведения, составляющие государственную тайну.					
6.1	Особенности обеспечения информационной безопасности создания и эксплуатации КСЗИ, обрабатывающей информацию, содержащую сведения, составляющие государственную тайну. /Тема/	10	0			
6.2	Требования к документированию КСЗИ, обрабатывающей информацию, содержащую сведения, составляющие государственную тайну (далее – государственная тайна): требования к документации; требования к среде разработки документации; требования к участникам разработки документации. Требования к среде разработки программного обеспечения КСЗИ, обрабатывающей государственную тайну. Требования к среде разработки информационного обеспечения КСЗИ, обрабатывающей государственную тайну. Требования к комплектации комплекса технических средств КСЗИ, обрабатывающих государственную тайну. Особенности проведения испытаний КСЗИ, обрабатывающей государственную тайну. /Лек/	10	2	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Конспект лекций.

6.3	Изучение конспекта лекций. /Ср/	10	2	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	подготовка конспекта по вопросам темы.
	Раздел 7. Иная контактная работа					
7.1	Иная контактная работа /Тема/	10	0			
7.2	Приём зачета. /ИКР/	10	0,25	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	Ответы на Контрольные вопросы Ответы на дополнительные вопросы.
	Раздел 8. Контроль					
8.1	Зачёт с оценкой /Тема/	10	0			
8.2	Подготовка к зачёту с оценкой /ЗаО/	10	8,75	ОПК-5.2.4-З ОПК-5.2.4-У ОПК-5.2.4-В ОПК-5.3.3-З ОПК-5.3.3-У ОПК-5.3.3-В	Л1.1 Л1.2 Л1.3Л2.1 Э1 Э2 Э3 Э4 Э5 Э6	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы приведены в приложении к рабочей программе дисциплины "Спецдисциплина 4" (см. документ "ОМ Спецдисциплина 4")

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.1	Чуянов А. Г., Симаков А. А.	Обеспечение информационной безопасности в компьютерных системах : учебное пособие	Омск: Омская академия МВД России, 2012, 204 с.	978-5-88651-535-0, http://www.iprbookshop.ru/36015.html
Л1.2	Жидко Е. А.	Логико-вероятностно-информационный подход к моделированию информационной безопасности объектов защиты : монография	Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2016, 121 с.	978-5-89040-614-9, http://www.iprbookshop.ru/72917.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.3	Душкин А. В., Барсуков О. М., Кравцов Е. В., Славнов К. В.	Программно-аппаратные средства обеспечения информационной безопасности	Москва: Горячая линия -Телеком, 2018, 248 с.	978-5-9912-0470-5, https://e.lanbook.com/book/111053

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Петров С. В., Кисляков П. А.	Информационная безопасность : учебное пособие	Саратов: Ай Пи Ар Букс, 2015, 326 с.	978-5-906-17271-6, http://www.iprbookshop.ru/33857.html

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронно-библиотечная система «Лань». – Режим доступа: доступ из корпоративной сети РГРТУ – свободный (без пароля).
Э2	Электронно-библиотечная система «IPRbooks». – Режим доступа: доступ из корпоративной сети РГРТУ – свободный (без пароля), доступ из сети Интернет – по паролю
Э3	Электронная библиотека РГРТУ. Режим доступа: из корпоративной сети РГРТУ – по паролю
Э4	Научная электронная библиотека eLibrary
Э5	Библиотека и форум по программированию
Э6	Национальный открытый университет ИНТУИТ

6.3 Перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование	Описание
Операционная система Windows	Коммерческая лицензия
Kaspersky Endpoint Security	Коммерческая лицензия
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
VMware Player	Свободное ПО

6.3.2 Перечень информационных справочных систем

6.3.2.1	Информационно-правовой портал ГАРАНТ.РУ http://www.garant.ru
6.3.2.2	Система КонсультантПлюс http://www.consultant.ru
6.3.2.3	Справочная правовая система «КонсультантПлюс» (договор об информационной поддержке №1342/455-100 от 28.10.2011 г.)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1	264 учебно-административный корпус. учебная аудитория для проведения учебных занятий Специализированная мебель (16 посадочных мест), 5 рабочих мест (стол), магнитно-маркерная доска.
2	268 учебно-административный корпус. компьютерный класс для проведения учебных занятий Специализированная мебель (20 компьютерных столов), 20 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методические указания обучающихся по освоению дисциплины приведены в документе, ссылка на который указана в разделе Приложения