

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Амурский государственный университет»

УТВЕРЖДАЮ  
Проректор по учебной работе

Н.В.Савина

«15»



**РАБОЧАЯ ПРОГРАММА**

**ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ  
ИНФОРМАЦИОННЫХ СИСТЕМ**

(наименование учебной дисциплины/модуля)

Направление подготовки 09.03.02 «Информационные системы и технологии»  
(шифр и наименование специальности/направления подготовки)

Направленность(профиль) образовательной программы «Безопасность информационных систем»

Квалификация выпускника Бакалавр

Программа подготовки академический бакалавриат

Год набора 2018

Форма обучения очная

Курс – 4

Семестр – 7, 8

Зачет – 7  
(семестр)

Экзамен – 8 (27 акад. час.)  
(семестр)

Лекции – 18(акад. час.) / 20(акад. час.)

Практические (семинарские) занятия – 18(акад. час.) / 20(акад. час.)

Самостоятельная работа – 72(акад. час.) / 113(акад. час.)

Общая трудоемкость дисциплины – 108(акад. час.) 3 з.е. / 180(акад. час.) 5 з.е.

Составители – С.Г. Самохвалова, доцент, канд. техн. наук;

Н.П. Семичевская, доцент, канд. техн. наук

(И.О.Ф., должность, ученое звание)

Факультет математики и информатики

Кафедра информационных и управляющих систем

2018 г.

Рабочая программа составлена на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии», утвержденного приказом Министерства образования и науки 12.03.2015 г., № 219

Рабочая программа обсуждена на заседании кафедры информационных и управляющих систем

« 15 » 05 2018 г., протокол № 9

Заведующий кафедрой  А.В. Бушманов  
подпись И.О.Ф.

Рабочая программа одобрена на заседании УМС направления подготовки  
09.03.02 «Информационные системы и технологии»

---

« 29 » 05 2018 г., протокол №9

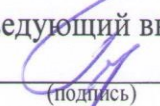
Председатель  А. В. Бушманов  
подпись И.О.Ф.

СОГЛАСОВАНО

Начальник учебно-методического  
управления  Н.А. Чалкина  
(подпись)

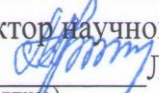
« 29 » 05 2018 г.

СОГЛАСОВАНО

Заведующий выпускающей кафедрой  
 А. В. Бушманов  
(подпись)

« 15 » 05 2018 г.

СОГЛАСОВАНО

Директор научной библиотеки  
 Л.А. Проказина  
(подпись)

« 29 » 05 2018 г.

## **1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**

### **Цель дисциплины (модуля):**

Цель преподавания дисциплины «Организационное и правовое обеспечение безопасности информационных систем» предоставить основные положения, понятия и определения правового обеспечения информационных систем, а также применению современных средств информационной безопасности. Программа дисциплины предназначена для реализации всех необходимых компетенций.

### **Задачи дисциплины (модуля):**

- изучение основных понятий и определений правового обеспечения информационной безопасности;
- изучение правовых норм в области обеспечения безопасности информационных систем;
- формирование устойчивых навыков практического использования юридических и правовых норм при сопровождении и эксплуатации информационных систем.

## **2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО**

Дисциплина относится к базовой части дисциплин Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии» (квалификация «бакалавр»).

Для успешного освоения данной дисциплины необходимы знания, умения и навыки, приобретенные в результате освоения дисциплин базовой Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии» (квалификация «бакалавр»): Правоведение, Информационные технологии.

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

В процессе освоения данной дисциплины студент формирует и демонстрирует следующие компетенции:

- знанием своих прав и обязанностей как гражданина своей страны, способностью использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии (ОК-9).
- пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4).

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

### **знать:**

- свои права и обязанности как гражданина своей страны, действующее законодательство и другие правовые документы в своей деятельности (ОК-9);
- сущность и значения информации в развитии современного информационного общества;

### **уметь:**

- использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии (ОК-9);
- соблюдать основные требования к информационной безопасности, в том числе защите государственной тайны (ОПК-4);

### **владеть:**

- знанием своих прав и обязанностей как гражданина своей страны, способностью использовать действующее законодательство и другие правовые документы в своей деятельности, демонстрировать готовность и стремление к совершенствованию и развитию общества на принципах гуманизма, свободы и демократии (ОК-9).

- пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4).

#### 4. МАТРИЦА КОМПЕТЕНЦИЙ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Раздел дисциплины	Компетенции	
		ОК-9	ОПК-4
<b>Семестр 7</b>			
1	Тема 1. Организационные системы обеспечения безопасности информации	+	+
2	Тема 2. Нормативные акты, служащие основанием для организационно-распорядительной документации по защите информации	+	+
3	Тема 3. Методики составления нормативной и методической документации по защите информации	+	+
4	Тема 4. Концепция построения системы безопасности предприятия	+	+
5	Тема 5. Организация и функции службы безопасности предприятия	+	+
6	Тема 6. Организация информационно-аналитической работы	+	+
7	Тема 7. Обеспечение безопасности информации на наиболее уязвимых направлениях деятельности предприятия	+	+
8	Тема 8. Методики составления методической документации по защите информации на наиболее уязвимых направлениях деятельности предприятия	+	+
9	Тема 9. Организация работы с персоналом предприятия	+	+
<b>Семестр 8</b>			
1	Тема 1. Правовые основы защиты информации	+	+
2	Тема 2. Стратегия национальной безопасности РФ	+	+
3	Тема 3. Структура Российского законодательства	+	+
4	Тема 4. Гражданский кодекс РФ	+	+
5	Тема 5. Кодекс об административных правонарушениях	+	+
6	Тема 6. Уголовный кодекс РФ	+	+
7	Тема 7. Федеральные законы РФ	+	+
8	Тема 8. Постановления, Указы Президента и Правительства РФ	+	+
9	Тема 9. Постановления, Указы Президента и Правительства РФ	+	+
10	Тема 10. Приказы, методические рекомендации органов исполнительной власти РФ	+	+

#### 5. СТРУКТУРА ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 акад. часов, в 7сем.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды контактной работы, включая самостоятельную работу студентов и трудоемкость в акад. часах			Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лек	Прак	Сам	
1	Тема 1. Организационные системы обеспечения безопасности информации	7	1	2	2	8	Отчет пр.раб.№1

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды контактной работы, включая самостоятельную работу студентов и трудоемкость в акад. часах			Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лек	Прак	Сам	
2	Тема 2. Нормативные акты, служащие основанием для организационно-распорядительной документации по защите информации	7	2	2	2	8	Отчет пр.раб.№2
3	Тема 3. Методики составление нормативной и методической документации по защите информации	7	3	2	2	8	Отчет пр.раб.№3
4	Тема 4. Концепция построения системы безопасности предприятия	7	4	2	2	8	Отчет пр.раб.№4
5	Тема 5. Организация и функции службы безопасности предприятия	7	5	2	2	8	Отчет пр.раб.№5
6	Тема 6. Организация информационно-аналитической работы	7	6	2	2	8	Отчет пр.раб.№6
7	Тема 7. Обеспечение безопасности информации на наиболее уязвимых направлениях деятельности предприятия	7	7	2	2	8	Отчет пр.раб.№7
8	Тема 8. Методики составления методической документации по защите информации на наиболее уязвимых направлениях деятельности предприятия	7	8	2	2	8	Отчет пр.раб.№8
9	Тема 9. Организация работы с персоналом предприятия	7	9	2	2	8	Отчет пр.раб.№9
Зачет		7					Подготовка к зачету
Всего по разделам		7	18	18	18	72	108

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 акад. часов, в 8 сем.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды контактной работы, включая самостоятельную работу студентов и трудоемкость в акад. часах			Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лек	Прак	Сам	

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды контактной работы, включая самостоятельную работу студентов и трудоемкость в акад. часах			Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лек	Прак	Сам	
1	<b>Раздел 1 Структура законодательства в области информации, информационных технологий и защиты информации</b> Тема1. Правовые основы защиты информации	8	1	2	2	10	Отчет пр.раб.№1 К.р. №1
2	Тема2. Стратегия национальной безопасности РФ	8	2	2	2	10	Отчет пр.раб.№2 К.р. №2
3	Тема3. Структура Российского законодательства	8	3	2	2	10	Отчет пр.раб.№3
4	<b>Раздел 2 Кодексы и законы (законодательные акты высшей юридической силы)</b> Тема4. Гражданский кодекс РФ	8	4	2	2	10	Отчет пр.раб.№4 К.р. №3
5	Тема5. Кодекс об административных правонарушениях	8	5	2	2	10	Отчет пр.раб.№5 К.р. №4
6	Тема6. Уголовный кодекс РФ	8	6	2	2	10	Отчет пр.раб.№6
7	Тема 7. Федеральные законы РФ		7	2	2	10	Отчет пр.раб.№7
8	Тема 8. Федеральные законы РФ	8	8	2	2	10	Отчет пр.раб.№8
9	Тема 9. Постановления, Указы Президента и Правительства РФ	8	9	2	2	10	Отчет пр.раб.№9
10	<b>Раздел 3 Иные нормативные документы</b> Тема 10. Приказы, методические рекомендации органов исполнительной власти РФ	8	10	2	2	10	Отчет пр.раб.№10 К.р. №5
Экзамен		8				27	Подготовка к итоговому тестированию
Всего по разделам		8	1-10	20	20	108	108

К.р. – контрольная работа, Пр.р. – практическая работа.

## 6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 6.1 Лекционные занятия 7-семестр

№	Темы лекций	Содержание лекции
1	2	3
1	Организационные системы обеспечения безопасности информации	Задачи и методы обеспечения ИБ в различных сферах деятельности. Организационные структуры государственной системы обеспечения ИБ федеральных органов исполнительной власти. Службы контроля и надзора органа исполнительной власти. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).
2	Нормативные акты, служащие основанием для организационно-распорядительной документации по защите информации	Корпоративная нормативная база по защите информации. Стандарты безопасности. Специальные требования и рекомендации по технической защите конфиденциальной информации. ФЗ «О техническом регулировании», понятие и требования аккредитации и сертификации. Политика безопасности. Анализ рисков. Перечень и содержание основных документов, необходимых при построении системы защиты в организации: приказы, распоряжения, перечни, матрицы, модели, акты, технические паспорта, схемы контролируемых зон, методические пособия, памятки, журналы. Перечень документов заявителя для аттестации автоматизированной системы и типовые формы. Некоторые рекомендации по проведению мероприятий по защите информации и выбору параметров защиты.
3	Концепция построения системы безопасности предприятия	Общая характеристика организационных методов защиты информации. Требования к построению систем безопасности предприятия. Концептуальная модель информационной безопасности. Виды объектов защиты. Характеристика защитных действий. Разглашение защищаемой информации. способы пресечения разглашения информации. Противодействие несанкционированному доступу к информации.
4	Организация и функции службы безопасности предприятия	Организация режима секретности, его особенности и содержание. Организационная служба безопасности. Организация внутриобъектового и пропускного режимов на предприятиях. Использование технических средств. Организация охраны предприятий.
5	Организация информационно-аналитической работы	Цели и задачи информационно-аналитической работы Направления и методы аналитической работы. Этапы выполнения информационно-аналитических исследований производственных ситуаций. Порядок деятельности по осуществлению требований организационно-распорядительной документации, периоды проверок, составы комиссий.
6	Обеспечение безопасности информации на наиболее уязвимых направлениях деятель-	Подготовка совещания по конфиденциальным вопросам. Выбор места проведения совещания. Организация охраны. Подготовка пропускного режима. Пропускной режим во время проведения совещания. Организация подготовки и

№	Темы лекций	Содержание лекции
1	2	3
	ности предприятия	проведения заседаний по конфиденциальным вопросам. Защита информации при работе с посетителями. Организация работы с документами.
7	Организация работы с персоналом предприятия	Принципы допуска персонала к различным видам документации. Ограниченный доступ персонала к компьютерной информации. Первичный инструктаж при приеме на работу. Периодический инструктаж. Периодическая учеба персонала.
8	Составление нормативной и методической документации по защите информации на предприятиях, эксплуатирующих ИС	Изучение действующих методик по составлению сводных таблиц и нормативных актов по защите информации на наиболее уязвимых направлениях деятельности предприятия. Перечень документов заявителя для аттестации автоматизированной системы и типовые формы. Некоторые рекомендации по проведению мероприятий по защите информации и выбору параметров защиты.

## 6.2 Практические занятия

### Темы практических занятий – 7 семестр

№	Темы занятий	Трудоемкость в акад. часах
1	<b>Практическое занятие №1</b> Изучение структуры государственной системы обеспечения информационной безопасности в РФ, основных нормативов и организационных документов, регламентирующих обращение с информацией ограниченного доступа.	2
2	<b>Практическое занятие №2</b> Разработка организационных мероприятий обеспечения информационной безопасности на режимном предприятии. Функции, задачи и особенности службы безопасности организации. Принципы организации службы безопасности организации. Типовая структура службы безопасности	2
3	<b>Практическое занятие №3</b> Допуск и доступ к конфиденциальной информации и документам. Организация подготовки и проведения совещания по конфиденциальным вопросам. Первичный инструктаж при приеме на работу. Периодический инструктаж. Периодическая учеба персонала	2
4	<b>Практическое занятие №4</b> Организация пропускного и внутриобъектового режима. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации. Требования к помещениям, в которых циркулирует защищаемая информация. 3. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима.	2
5	<b>Практическое занятие №5</b> Требования режима секретности при работе с секретными документами. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов. Формы допусков. Служебное рас-	2



№	Темы занятий	Трудо- емкость в акад. часах
	следование нарушений режима секретности.	
6	<b>Практическое занятие №6</b> Организация и обеспечение режима секретности. Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве.	2
7	<b>Практическое занятие №7</b> Составление инструкций с требованиями режима секретности при работе с секретными документами.	3
8	<b>Практическое занятие №8</b> Служебное расследование нарушений режима секретности. Организация работ по защите информации при опубликовании открытых материалов.	3
Итого		18

### 6.3 Лекционные занятия 8-семестр

№	Темы лекций	Содержание лекции
1	2	3
<b>Раздел 1 Структура Российского законодательства в области информации, информационных технологий и защиты информации</b>		
1	<b>Тема 1.</b> Правовые основы защиты информации	Виды, типы информации (понятие информации в различных законах). Основные цели и задачи служб защиты информации (безопасности). Структура организационно-правового обеспечения. Аспекты системы защиты информации: организационные, технико-математические и юридические. Особенности организационно-правового обеспечения защиты информации в АС.
2	<b>Тема 2.</b> Стратегия национальной безопасности РФ	Международное законодательство: резолюции, конвенции. Доктрина информационной безопасности.
3	<b>Тема 3.</b> Структура Российского законодательства	Структура правового обеспечения информации и защиты информации в РФ. Нормативно-правовые акты в области информационной безопасности: Международные договоры РФ; Конституция РФ; Кодексы РФ; Законы федерального уровня (включая федеральные конституционные законы, кодексы); Указы Президента РФ; Постановления правительства РФ; Нормативные правовые акты федеральных министерств и ведомств; Нормативные правовые акты субъектов РФ, органов местного самоуправления; Нормативно-методические документы
<b>Раздел 2 Кодексы и законы (законодательные акты высшей юридической силы)</b>		
4	<b>Тема 4.</b> Кодексы РФ	Статьи гражданского кодекса. Статьи кодекса об административных правонарушениях. Статьи уголовного кодекса. Статьи трудового кодекса.

№	Темы лекций	Содержание лекции
1	2	3
5	<b>Тема5.</b> Федеральные законы РФ	№ 149 – ФЗ «Об информации, информационных технологиях и защите информации»; № 390-ФЗ «О безопасности»; № 152 – ФЗ «О персональных данных»; № 63 – ФЗ "Об электронной подписи"; № 98– ФЗ «О коммерческой тайне»; № __ – ФЗ «О государственной тайне»
6	<b>Тема6.</b> Постановления, Указы Президента и Правительства РФ	Указы и распоряжения Президента Российской Федерации <b>Постановления Правительства Российской Федерации:</b> от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»; от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»; от 03 февраля 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;
<b>Раздел 3 ГОСТы, стандарты и другие нормативные акты</b>		
7	<b>Тема7.</b> Приказы, методические рекомендации органов исполнительной власти РФ	Методические документы государственных органов России: Руководящие документы ФСТЭК (Гостехкомиссии России); Приказы ФСБ; Стандарты информационной безопасности, из которых выделяют: Международные стандарты; Государственные (национальные) стандарты РФ; Рекомендации по стандартизации; Методические указания.

#### 6.4 Практические занятия

##### Темы практических занятий – 8 семестр

№	Темы занятий	Трудоемкость в акад. часах
1	<b>Практическое занятие №1</b> Структура Российского законодательства в области информации, информационных технологий и защиты информации	2
2	<b>Практическое занятие №2</b> Статьи Гражданского кодекса РФ в области ИТ и ИБ.	2
3	<b>Практическое занятие №3</b> Статьи Кодекса об административных правонарушениях РФ в области ИТ и ИБ.	2
4	<b>Практическое занятие №4</b> Статьи Уголовного кодекса РФ в области ИТ и ИБ.	2
5	<b>Практическое занятие №5</b> № 149 – ФЗ «Об информации, информационных технологиях и защите информации»	2

№	Темы занятий	Трудоемкость в акад. часах
6	<b>Практическое занятие №6</b> № 152 – ФЗ «О персональных данных»	2
7	<b>Практическое занятие №7</b> № 63 – ФЗ «Об электронной подписи»	2
8	<b>Практическое занятие №8</b> Российские государственные стандарты для унифицированного алгоритмического обеспечения средств криптографической защиты	2
9	<b>Практическое занятие №9</b> Государственные (национальные) стандарты РФ	2
10	<b>Практическое занятие №10</b> Документы ФСБ, ФСТЭК и Роскомнадзора.	2
Итого		20

## 7. САМОСТОЯТЕЛЬНАЯ РАБОТА

Семестр -7

№ п/п	№ раздела (темы) дисциплины	Форма (вид) самостоятельной работы	Трудоёмкость в академических часах
1	2	3	4
1	Организационные системы обеспечения безопасности информации	Работа с лекционным материалом.	10
2	Нормативные акты, служащие основанием для организационно-распорядительной документации по защите информации	Подготовка к практическим занятиям, подготовка к опросу	10
3	Концепция построения системы безопасности предприятия	Работа с лекционным материалом. Подготовка к лабораторной работе	12
4	Организация и функции службы безопасности предприятия	Работа с лекционным материалом. Подготовка к опросу	10
5	Организация информационно-аналитической работы	Подготовка к практическим и лабораторным занятиям, подготовка к опросу. Подготовка к лабораторной работе	10
6	Обеспечение безопасности информации на наиболее уязвимых направлениях деятельности предприятия	Работа с лекционным материалом Подготовка к практическим занятиям, подготовка к тесту	10

7	Организация работы с персоналом предприятия	Работа с лекционным материалом. Подготовка к практическим занятиям. Подготовка к тесту	10
ИТОГО			72

**Семестр -8**

№ п/п	Раздел дисциплины	Форма (вид) самостоятельной работы	Трудоемкость в акад. часах
1	<b>Раздел 1</b> Тема. Структура Российского законодательства в области защиты информации в ИС	Работа с учебной, справочной и нормативной литературой. Подготовка отчета. Контрольная работа №1 «Система информационного права в области защиты информации» Контрольная работа №2 «Перечень национальных концепций РФ информационной безопасности»	36
2	<b>Раздел 2</b> Тема. Федеральные законы РФ	Работа с учебной справочной и нормативной литературой. Подготовка отчета. Контрольная работа №3 «ФЗ №149 «Об информации, информационных технологиях и о защите информации» Контрольная работа №4 ФЗ от 09.02.2009 N 8-ФЗ (ред. от 28.12.2015) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»	36
3	<b>Раздел 3</b> <b>Тема.</b> Постановления, Указы Президента и Правительства РФ <b>Тема.</b> ГОСТы и стандарты криптографической защиты	Работа с учебной справочной и нормативной литературой. Подготовка отчета. Контрольная работа №5 ФЗ от 27.07.2006 N 152-ФЗ (ред. от 21.12.2015) «О персональных данных»	41
4	Экзамен	Подготовка к итоговому тестированию	27 акад. час.
Итого			113+27

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

7.1 Учебно-методическое обеспечение самостоятельной работы

7.1.1 Учебно-методическое пособие по дисциплине Методы и средства защиты компьютерной информации [Электронный ресурс]/ — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2016.— 32 с.— Режим доступа: <http://www.iprbookshop.ru/61498>. — ЭБС «IPRbooks»

7.1.2 Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Элек-

трон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: <http://www.iprbookshop.ru/62945.html>. — ЭБС «IPRbooks»

## 8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе подготовки по дисциплине используется совокупность методов и средств обучения, позволяющих осуществлять целенаправленное методическое руководство учебно-познавательной деятельностью магистрантов, в том числе на основе интеграции информационных и традиционных педагогических технологий.

При реализации настоящей рабочей программы предусматриваются интерактивные и активные формы проведения занятий, дискуссии по темам исследования и поставленным научным проблемам

### *Методы и формы организации обучения (ФОО)*

ФОО	Лекция	Лаб. раб.	Пр. зан./ Сем.,	СРС
Методы				
IT-методы	+		+	+
Работа в команде			+	
Case-study				+
Методы проблемного обучения.	+			
Опережающая самостоятельная работа				+
Поисковый метод				+
Другие методы	+		+	

Объем занятий, проводимых в интерактивных формах, составляет 12 академических часов аудиторных занятий.

Тема	Вид занятия	Кол-во академических часов
Организационные системы обеспечения безопасности информации	IT-методы	4
Нормативные акты, служащие основанием для организационно-распорядительной документации по защите информации	Проблемная лекция	2
Организация работы с персоналом предприятия	Работа в команде	2
Организация и функции службы безопасности предприятия	Метод проектов	2
Организация информационно-аналитической работы	IT-методы	2
		12

Рекомендуется использование информационных технологий при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа-средств при проведении лекционных и лабораторных занятий.

Образовательный процесс по дисциплине строится на основе комбинации следующих образовательных технологий.

Интегральную модель образовательного процесса по дисциплине формируют технологии методологического уровня: модульно-рейтинговое обучение, технология поэтапного формирования умственных действий, технология развивающего обучения, элементы технологии развития критического мышления. Реализация данной модели предполагает использование следующих технологий стратегического уровня (задающих организацион-

ные формы взаимодействия субъектов образовательного процесса), осуществляемых с использованием определенных тактических процедур:

- лекционные (вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция);
- лабораторные (углубление знаний, полученных на теоретических занятиях, программирование и компьютерное моделирование);
- самоуправления (самостоятельная работа студентов, самостоятельное изучение материала, подготовка к отчетным мероприятиям);
- электронная форма обучения, представленная электронными учебными материалами, тестовыми заданиями в электронном виде, подсистемой управления компетенциями для отслеживания результатов обучения, системой интерактивной поддержки обучающей среды, системой управления знаниями, системой управления обучением.

Также формируется **портфолио** компетенций, работающего в ЭО сотрудника, системы управления содержанием (контентом) обучения, системы доставки учебных материалов «в нужное время в нужном количестве в нужное место», системы тестирования, создаются электронные средства обучения, организации и сопровождения учебного процесса, отрабатываются различные **модели управления электронным обучением**, разрабатываются подходы к **оценке качества и эффективности ЭО**.

Рекомендуется использование информационных технологий при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа-средств при проведении лекционных и практических занятий.

Удельный вес занятий, проводимых в интерактивной форме в 8 семестре согласно требованиям Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 09.03.02 «Информационные системы и технологии» (квалификация «бакалавр») должен составлять:

№ п/п	Раздел дисциплины	Форма (вид) образовательных технологий	Количество акад. часов
1	Тема 1	Мультимедийная лекция	2
2	Тема 3	Мультимедийная лекция	2
3	Тема 5	Практическое занятие	2
4	Тема 9	Практическое занятие	2
5	Всего по разделам		8

## **9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания, типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций, а также методические материалы, определяющие процедуры оценивания знаний, умений и навыков по дисциплине «Организационное и правовое обеспечение безопасности информационных систем».

### **9.1 Оценочные средства для текущего контроля успеваемости**

#### **Перечень вопросов к зачету**

#### **7 –семестр**

1. Государственная система защиты информации в РФ от иностранных технических разведок и от ее утечки по техническим каналам.

2. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа.

3. Оценка соответствия объектов информатизации требованиям безопасности информации.
4. Классификация автоматизированных систем и требования по защите информации.
7. Организационные средства защиты информации. Место организационных средств в систем комплексной защиты информации объектов информатизации. Классификация и основное содержание направлений организационной деятельности по обеспечению информационной безопасностью
8. Архитектура систем защиты информации. Классификация требований к СЗИ. Принципы построения систем защиты.
9. Служба защиты информации. Нормативная база создания служб защиты информации. Принципы организации службы. Основные задачи службы. Функции службы защиты информации. Порядок взаимодействия службы защиты информации с другими структурными подразделениями объекта.
10. Общее содержание организации и обеспечения работ по защите информации. Основные мероприятия по подготовке лиц, ответственных за обеспечение информационной безопасности. Управление процессами функционирования систем защиты информации.
11. Организационное и документальное обеспечение работ по защите информации. Основное назначение документационного обеспечения информационной безопасности. Структура и состав системы документационного обеспечения защиты информации.
12. Организация пропускного и внутриобъектового режима. Понятие "пропускной режим". Основные мероприятия по обеспечению пропускного режима на объекте. Средства технического контроля и управления доступом.
13. Понятия государственной, профессиональной, служебной тайны. Конфиденциальная информация. Признаки информации, составляющей коммерческую тайну.
14. Человеческий фактор в системе защиты информации. Способы мотивации сотрудников. Формы сотрудничества со злоумышленниками.
15. Методы противодействия разглашению ценной информации. Начальная и текущая стадии взаимодействия сотрудника и организации. Методы подбора персонала с точки зрения обеспечения ИБ. Мотивация.
16. Понятие политики информационной безопасности, принципы разработки и внедрения эффективных политик.
17. Организация и поддержание конфиденциального документооборота. Программные, аппаратные и организационные средства его обеспечения.

### **Перечень вопросов к экзамену**

**8 -семестр**

#### **Раздел 1 Структура Российского законодательства в области информации, информационных технологий и защиты информации**

1. Виды, типы информации (понятие информации в различных законах).
2. Основные цели и задачи служб защиты информации (безопасности).
3. Структура организационно-правового обеспечения. Аспекты системы защиты информации: организационные, технико-математические и юридические.
4. Особенности организационно-правового обеспечения защиты информации в АС.
5. Международное законодательство: резолюции, конвенции.
6. Доктрина информационной безопасности.
7. Международные договоры РФ.
8. Конституция РФ;

#### **Раздел 2 Кодексы и законы (законодательные акты высшей юридической силы)**

9. Статьи Гражданского кодекса РФ.
10. Статьи Кодекса об административных правонарушениях.
11. Статьи Уголовного кодекса.
12. Статьи трудового кодекса.

13. № 149 – ФЗ «Об информации, информационных технологиях и защите информации»
14. № 390 -ФЗ «О безопасности»
15. № 152 – ФЗ «О персональных данных»
16. № 63 – ФЗ «Об электронной подписи»
17. Указы и распоряжения Президента Российской Федерации
18. Постановления Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»
19. от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

### **Раздел 3 ГОСТы, стандарты и другие нормативные акты**

19. Руководящие документы ФСТЭК (Гостехкомиссии России)  
Информационное сообщение ФСТЭК России от 6 апреля 2015 г. № 240/13/357 [«О новой редакции перечней технической \(технологической\) документации национальных стандартов и методических документов...»](#)
20. Информационное сообщение ФСТЭК России от 15 июля 2013 г. № 240/22/2637 [«По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах...»](#)
22. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 [«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»](#)
23. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 [«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»](#)
24. ФСТЭК России от 11 февраля 2014 г. Методический документ [«Меры защиты информации в государственных информационных системах»](#)
25. Документы ФСБ  
Приказ ФСБ России от 10.07.2014 N 378  
«Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 N 33620)
26. Документы Роскомнадзора  
Приказ Россвязькомнадзора № 996 от 05 сентября 2013 г. [«Об утверждении требований и методов по обезличиванию персональных данных»](#);
27. Приказ Россвязькомнадзора № 08 от 17 июля 2008 г. [«Об утверждении образца формы уведомления об обработке персональных данных»](#)
28. Национальные стандарты в области информационной безопасности  
[Перечень Государственных стандартов Российской Федерации в области защиты конфиденциальной информации и персональных данных](#)
29. Государственные (национальные) стандарты РФ  
ГОСТ ИСО 7498-2 99 Информационная технология. ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ. БАЗОВАЯ ЭТАЛОННАЯ МОДЕЛЬ



30. ГОСТ Р ИСО/МЭК 15408-1 2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
31. ГОСТ Р ИСО/МЭК 15408-2 2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
32. ГОСТ Р ИСО/МЭК 15408-3 2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
33. ГОСТ ИСО/МЭК 17789 2005 Информационная технология практические правила управления информационной безопасностью
34. Российские государственные стандарты для унифицированного алгоритмического обеспечения средств криптографической защиты  
ГОСТ Р 34.10 - 94 «Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» (ГОСТ Р 34.10 – 2001, ГОСТ Р 34.10 - 2012)
35. ГОСТ Р 34.11 - 94 «Информационная технология. Криптографическая защита информации. Функция хэширования» (ГОСТ Р 34.11 - 2012)

## **10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

### **а) основная литература**

1. Аверченков В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: <http://www.iprbookshop.ru/7002>. — ЭБС «IPRbooks»

2. Аверченков В.И. Служба защиты информации. Организация и управление [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 186 с.— Режим доступа: <http://www.iprbookshop.ru/7008>. — ЭБС «IPRbooks»

3. Аверченков В.И. Системы организационного управления [Электронный ресурс]: учебное пособие/ Аверченков В.И., Ерохин В.В.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 208 с.— Режим доступа: <http://www.iprbookshop.ru/7013>. — ЭБС «IPRbooks»

4. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 с.— Режим доступа: <http://www.iprbookshop.ru/43960.html>. — ЭБС «IPRbooks»

5. Кремер А.С. Нормативно-правовые аспекты обеспечения информационной безопасности инфокоммуникационных сетей [Электронный ресурс]: учебное пособие/ Кремер А.С.— Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2007.— 97 с.— Режим доступа: <http://www.iprbookshop.ru/61745.html>. — ЭБС «IPRbooks»

### **б) дополнительная литература**

1. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 с.— Режим доступа: <http://www.iprbookshop.ru/52160>. — ЭБС «IPRbooks»

3. Учебно-методическое пособие по дисциплине Методы и средства защиты компьютерной информации [Электронный ресурс]/ — Электрон. текстовые данные.— М.: Мос-

ковский технический университет связи и информатики, 2016.— 32 с.— Режим доступа: <http://www.iprbookshop.ru/61498>. — ЭБС «IPRbooks»

4. Качановский Ю.П. Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами [Электронный ресурс]: методические указания к проведению лабораторной работы по курсу «Информатика»/ Качановский Ю.П., Широков А.С.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2014.— 24 с.— Режим доступа: <http://www.iprbookshop.ru/55120>. — ЭБС «IPRbooks»

5. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: <http://www.iprbookshop.ru/43183>. — ЭБС «IPRbooks»

6. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: <http://www.iprbookshop.ru/10677>. — ЭБС «IPRbooks»

7. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: <http://www.iprbookshop.ru/6991>. — ЭБС «IPRbooks»

8. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: <http://www.iprbookshop.ru/62945.html>. — ЭБС «IPRbooks»

#### Нормативно–техническая документация

1. Конституция РФ
2. Кодекс гражданский
3. Кодекс об административных правонарушениях
4. Кодекс уголовный
5. Федеральный закон № 149 – ФЗ «Об информации, информационных технологиях и защите информации»
6. Федеральный закон № 98 – ФЗ «О коммерческой тайне»
7. Федеральный закон № \_\_ – ФЗ «О государственной тайне»
8. Федеральный закон № 152 – ФЗ «О персональных данных»
9. Федеральный закон № 63 – ФЗ "Об электронной подписи"
10. ГОСТы и стандарты, положения ФСТЭК и ФСБ

#### г) программное обеспечение и Интернет-ресурсы

**7 семестр**

№	Наименование ресурса	Краткая характеристика
1	<a href="http://www.iprbookshop.ru/">http://www.iprbookshop.ru/</a>	Электронно-библиотечная система IPRbooks – научно-образовательный ресурс для решения задач обучения в России и за рубежом. Уникальная платформа ЭБС IPRbooks объединяет новейшие информационные технологии и учебную лицензионную литературу. Контент ЭБС IPRbooks отвечает требованиям стандартов высшей школы, СПО, дополнительного и дистанционного образования. ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования

2	<a href="http://www.itsec.ru">http://www.itsec.ru</a>	Электронный журнал по информационной безопасности.
3	<a href="http://elibrary.ru">http://elibrary.ru</a>	Научная электронная библиотека журналов
4	<a href="http://all-ib.ru/content/osnovi-zasiti-informacii/osnovi_zasiti_informacii_part_1.html">http://all-ib.ru/content/osnovi-zasiti-informacii/osnovi_zasiti_informacii_part_1.html</a>	Организационные основы защиты информации на предприятии
5	<a href="http://iintb.rggu.ru/section.html?id=2786">http://iintb.rggu.ru/section.html?id=2786</a>	Институт информационных наук и технологий безопасности
6	MS Windows 10	Операционная система MS Windows 10 Education - DreamSpark Premium Electronic Software Delivery (3 years) Renewal по договору - Сублицензионный договор № Tr000074357/КНВ 17 от 01 марта 2016 года
7	LibreOffice	Пакет прикладных программ, бесплатное распространение по лицензии MozillaPublicLicenseVersion 2.0 <a href="http://www.libreoffice.org/download/license/">http://www.libreoffice.org/download/license/</a>

### 8 семестр

№	Наименование ресурса	Краткая характеристика
1	<a href="http://www.iprbookshop.ru">http://www.iprbookshop.ru</a>	ЭБС IPRbooks — научно-образовательный ресурс для решения задач обучения в России и за рубежом. Уникальная платформа ЭБС IPRbooks объединяет новейшие информационные технологии и учебную лицензионную литературу. Контент ЭБС IPRbooks отвечает требованиям стандартов высшей школы, СПО, дополнительного и дистанционного образования. ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования
2.	<a href="https://e.lanbook.com/">https://e.lanbook.com/</a>	Электронно-библиотечная система ЛАНЬ
3.	<a href="http://gostedu.ru">http://gostedu.ru</a>	ГОСТы, СНИПы, СанПиНы и др. образоват. ресурсы

#### Программное обеспечение (лицензии на ПО)

№	Наименование ресурса	Краткая характеристика
1.	Операционная система MS Windows 10 Education	DreamSpark Premium Electronic Software Delivery (3 years) Renewal по договору - Сублицензионный договор № Tr000074357/КНВ 17 от 01 марта 2016 года
2.	MS Office 2010 standard	лицензия Microsoft office 2010 Standard RUS OLP ML Academic 50, договор №492 от 28 июня 2012 года
3.	Google Chrome	Бесплатное распространение по лицензии google chromium <a href="http://code.google.com/intl/ru/chromium/terms.html">http://code.google.com/intl/ru/chromium/terms.html</a>
4.	Программный комплекс «КонсультантПлюс»	лицензия коммерческая по договору №21 от 29 января 2015 года
5.	Автоматизированная информационная библиотечная система «ИРБИС 64»	лицензия коммерческая по договору №945 от 28 ноября 2011 года

## 11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении дисциплины применяется рейтинговая технология обучения, которая позволяет реализовать непрерывную и комплексную систему оценивания учебных достижений студентов. Непрерывность означает, что текущие оценки не усредняются, а непрерывно складываются на протяжении одного семестра. Комплексность означает учет всех форм учебной и творческой работы студента в течение семестра.

Рейтинг направлен на повышение ритмичности и эффективности самостоятельной работы студентов. Он основывается на заинтересованности каждого студента в получении более высокой оценки знаний по дисциплине.

Принципы рейтинга: непрерывный контроль и получение более высокой оценки за работу, выполненную в срок.

Рейтинг включает в себя три вида контроля: текущий, промежуточный и итоговый по дисциплине.

Текущий контроль – это опросы на семинарах по пройденным темам.

Опросы проводятся на каждом семинаре по содержанию лекционного материала, а также по базовым знаниям, полученным на практических занятиях.

#### **Методические рекомендации по организации и проведению тестирования**

Использование тестовых заданий возможно при всех видах контроля. Оптимальным является применение тестов в сочетании с другими формами контроля. Это обеспечивает максимально объективные оценки, как усвоению содержания обучения, так и мыслительной деятельности студента. Традиционно в высшем образовании широко применяется методика объективного контроля, основанная на различиях в уровне усвоения нового материала. Данная методика различает тесты 3 уровней. Первый уровень направлен на узнавание ранее изученного материала. При текущем контроле используются тесты первого уровня.

Тесты второго уровня также являются репродуктивными, но в их заданиях не содержится материала для ответа (тест на подставку, конструктивный тест, типовая задача с типичными условиями, и ее решение достигается ранее изученным достаточно простым методом). Третий уровень – нетиповые задачи повышенной сложности, для решения которых требуется самостоятельное нахождение методов решения. Эта методика успешно может применяться при проведении входного контроля, можно ее использовать и при текущем контроле.

#### **Описание критериев оценки на зачете – 7 семестр:**

**Критерии оценки тестовых работ:** оценка «зачтено» выставляется студенту, если количество правильных ответов составляет 50 и более процентов; оценка «не зачтено» выставляется студенту, если количество правильных ответов менее 50%.

#### **Описание критериев оценки на экзамене – 8 семестр:**

Диапазон оценки промежуточного контроля дисциплины от «неудовлетворительно» до «отлично».

зачет с оценкой «**отлично**» выставляется магистранту, если его отчет по тестовому заданию содержит от 90% – 100% правильных ответов;

зачет с оценкой «**хорошо**» выставляется студенту, если его отчет по тестовому заданию содержит от 70% – 90% правильных ответов;

зачет с оценкой «**удовлетворительно**» выставляется студенту, если его отчет по тестовому заданию содержит от 50% – 69% правильных ответов;

зачет с оценкой «**неудовлетворительно**» выставляется студенту, если его отчет по тестовому заданию содержит менее 50% правильных ответов.

## **11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Занятия по дисциплине проводятся в специальных помещениях, представляющих собой учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Все помещения, в которых проводятся занятия, соответствуют действующим противопожарным правилам и нормам.

Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам и к электронной информационно-образовательной среде университета.

Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета

Лекции и практические занятия проводятся в лекционной аудитории, оборудованной проектором, экраном, учебной доской, ноутбуком.

В качестве основных технических средств обучения по дисциплине в 8 – семестре используются:

12.1 Лекционная аудитория, оборудованная мультимедиа средствами, для проведения занятий в дистанционной, мультимедийной и электронной формах.

12.2 Аудитория оборудованная мультимедиа средствами, для проведения лабораторных занятий в мультимедийной и электронной формах.

12.3 Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.