ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.18. Техническая защита информации

Направление подготовки (специальность)
09.03.01 Информатика и вычислительная техника

Профиль подготовки (специализация)
"Автоматизированные системы обработки информации и управления**"**

Квалификация (степень) выпускника бакалавр

Форма обучения очная

1. Цели освоения дисциплины

Дисциплина «Техническая защита информации» имеет целью раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование основных практических навыков работы в данной области.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Б1.В.18. Техническая защита информации» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Б1.В.18. Техническая защита информации» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Дисциплина	Раздел
Основы информационной безопасности	Все разделы

Таблица 2.2 – Требования к постреквизитам дисциплины

Дисциплина	Раздел
Техническая защита информации	Все разделы

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в	Этап 1: Технология разработки политики ИБ АС Этап 2: Технология разработки политики ИБ АС	Этап 1: Разработка политики ИБ АС Этап 2: Умение работать с политикой ИБАС	Этап 1: Теоретический опыт разработки политики ИБ АС Этап 2: Практический опыт разработки политики ИБ АС

области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства **(ОК-5)**			
способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности **(ПК-31)**	Этап 1: Технология проектирования системы управления ИБ АС Этап 2: Технология использования системы управления ИБ АС	Этап 1: Проектирование системы управления ИБ АС Этап 2: Проектирование системы управления ИБ АС	Этап 1: Теоретический опыт проектирования системы управления ИБ АС Этап 2: Практический опыт проектирования системы управления ИБ АС
способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите **(ПК-32)**	Этап 1: Теоретические основы проведения экспериментов Этап 2: Практические основы проведения экспериментов	Этап 1: Проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации Этап 2: Проведение экспериментально-исследовательских работ при	Этап 1: Теоретический опыт проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации Этап 2: Практический опыт проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных

		аттестации АС без учета нормативных требований по защите информации	требований по защите информации

4. Объем дисциплины

Объем дисциплины «Б1.В.18. Техническая защита информации» составляет 3 зачетные единицы (108 академических часов), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр №6	
				КР	СР
1	**2**	**3**	**4**	**7**	**8**
1	Лекции (Л)	18		18	
2	Лабораторные работы (ЛР)				
3	Практические занятия (ПЗ)	34		34	
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)				
10	Подготовка к занятиям (ПкЗ)		54		54
11	Промежуточная аттестация	2		2	
12	Наименование вида промежуточной аттестации			Зачет	
13	Всего	54	54	54	54

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	**Раздел 1 Основные понятия и определения**	**4**	**4**		**8**						14		**ОК-5 ПК-31/32**
1.1.	**Тема 1** Термины и определения в области технической защиты информации	4	2		4						7		**ОК-5 ПК-31/32**
1.2.	**Тема 2** Классификация технических каналов утечки информации	4	2		4						7		**ОК-5 ПК-31/32**
2.	**Раздел 2 Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами**	**4**	**4**		**8**						14		**ОК-5 ПК-31/32**
2.1.	**Тема 3** Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	4	2		4						7		**ОК-5 ПК-31/32**
2.2.	**Тема 4** Виды каналов утечки информации	4	2		4						7		**ОК-5 ПК-31/32**
3.	**Раздел 3 Системный подход к инженерно-технической защите информации**	**4**	**4**		**8**						14		**ОК-5 ПК-31/32**
3.1.	**Тема 5**	4	2		4						7		**ОК-5**

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
	Способы и средства защиты информации обрабатываемой средствами вычислительной техники и автоматизированными системами												**ПК-31/32**
3.2.	**Тема 6** Способы и средства зашиты выделенных помещений от утечки речевой информации по техническим каналам	4	2		4						7		**ОК-5 ПК-31/32**
4.	**Раздел 4 Основные этапы проектирования системы защиты информации техническими средствами**	**4**	**6**		**12**						12		**ОК-5 ПК-31/32**
4.1.	**Тема 7** Организация технической защиты информации	4	2		6						6		**ОК-5 ПК-31/32**
4.2.	**Тема 8** Лицензирование деятельности по технической защите информации	4	4		4						6		**ОК-5 ПК-31/32**
5.	**Контактная работа**	**4**	**18**		**34**							**2**	
6.	**Самостоятельная работа**	**4**									**54**		
7.	**Объем дисциплины в семестре**	**4**	**18**		**34**						**54**		
8.	**Всего по дисциплине**		**18**		**34**						**54**		

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Термины и определения в области технической защиты информации	2
Л-2	Классификация технических каналов утечки информации	2
Л-3	Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	2
Л-4	Виды каналов утечки информации	2
Л-5	Способы и средства защиты информации обрабатываемой средствами вычислительной техники и автоматизированными системами	2
Л-6	Способы и средства зашиты выделенных помещений от утечки речевой информации по техническим каналам	2
Л-7	Организация технической защиты информации	2
Л-8	Лицензирование деятельности по технической защите информации	4
Итого по дисциплине		18

5.2.2 – Темы лабораторных работ (не предусмотрены учебным планом)

5.2.3 – Темы практических занятий

№ п.п.	Наименование темы занятия	Объем, академические часы
ПЗ-1	Термины и определения в области технической защиты информации	4
ПЗ-2	Классификация технических каналов утечки информации	4
ПЗ-3	Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	4
ПЗ-4	Виды каналов утечки информации	4
ПЗ-5	Способы и средства защиты информации обрабатываемой средствами вычислительной техники и автоматизированными системами	4
ПЗ-6	Способы и средства зашиты выделенных помещений от утечки речевой информации по техническим каналам	4
ПЗ-7	Организация технической защиты информации	6
ПЗ-8	Лицензирование деятельности по технической защите информации	4
Итого по дисциплине		34

5.2.4 – Темы семинарских занятий (не предусмотрены учебным планом)

5.2.5 Темы курсовых работ (проектов) (не предусмотрены учебным планом)

5.2.6 Темы рефератов (не предусмотрены)

5.2.7 Темы эссе (не предусмотрены)

5.2.8 Темы индивидуальных домашних заданий (не предусмотрены)

5.2.9 – Вопросы для самостоятельного изучения (не предусмотрены)

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Основная литература, необходимая для освоения дисциплины

1. Галатенко. В.А. Основы информационной безопасности [электронный ресурс]: курс лекций: учебное пособие / под ред. В.Б. Бетелина. Издательство: Интернет-Университет Информационных Технологий. 2006. - 208 с. http://www.knigafund.ru/

2. Галатенко. В.А. Стандарты информационной безопасности: курс лекций: учебное пособие. Издательство Основы информационной безопасности [электронный ресурс]: Интернет-Университет Информационных Технологий, 2006 264 с. http ://www. knigafund. ru/

6.2. Дополнительная литература, необходимая для освоения дисциплины

1. Попов, В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности Основы информационной безопасности [электронный ресурс]: Учебное пособие Издательство: Финансы и статистика, 2005. - 174 с. http://www.knigafund.ru/ '

2. Лапонина. О.Р. Межсетевое экранирование Основы информационной безопасности [электронный ресурс]: Учебное пособие. Издательство: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2007 - 344 с. http://www.knigafund.ru/

6.3. Методические указания для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие включающее:
- конспект лекций;
- методические указания по выполнению практических работ.

6.4 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Windows XP
2. Windows 7
3. Open Office

6.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.knigafund.ru/ - ЭБС
2. http://e.lanbook.com/ - ЭБС
3. http://rucont.ru/ - ЭБС
4. http://elibrary.ru/defaultx.asp - ЭБС
5. http://www.rsl.ru Российская государственная библиотека (РГБ)
6. http://www.edu.ru/ - федеральный портал российского образования

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

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение практических занятий

№ п.п.	Наименование темы	Название специализированной лаборатории	Название спецобору дования	Название технических и электронных средств обучения и контроля знаний
ПЗ-1	Термины и определения в области технической защиты информации	953 лаборатория интеллектуальных систем, 957 лаборатория аппаратных средств вычислительной системы	ПЭВМ	Windows XP Windows 7 Open Office
ПЗ-2	Классификация технических каналов утечки информации	953 лаборатория интеллектуальных систем, 957 лаборатория аппаратных средств вычислительной системы	ПЭВМ	Windows XP Windows 7 Open Office
ПЗ-3	Общая характеристика и классификация технических каналов утечки информации, обрабатываемой	953 лаборатория интеллектуальных систем, 957 лаборатория аппаратных средств вычислительной системы	ПЭВМ	Windows XP Windows 7 Open Office

	средствами вычислительной техники и автоматизированными системами			
ПЗ-4	Виды каналов утечки информации	953 лаборатория интеллектуальных систем, 957 лаборатория аппаратных средств вычислительной системы	ПЭВМ	Windows XP Windows 7 Open Office
ПЗ-5	Способы и средства защиты информации обрабатываемой средствами вычислительной техники и автоматизированными системами	953 лаборатория интеллектуальных систем, 957 лаборатория аппаратных средств вычислительной системы	ПЭВМ	Windows XP Windows 7 Open Office
ПЗ-6	Способы и средства зашиты выделенных помещений от утечки речевой информации по техническим каналам	953 лаборатория интеллектуальных систем, 957 лаборатория аппаратных средств вычислительной системы	ПЭВМ	Windows XP Windows 7 Open Office
ПЗ-7	Организация технической защиты информации	953 лаборатория интеллектуальных систем, 957 лаборатория аппаратных средств вычислительной системы	ПЭВМ	Windows XP Windows 7 Open Office
ПЗ-8	Лицензирование деятельности по технической защите информации	953 лаборатория интеллектуальных систем, 957 лаборатория аппаратных средств вычислительной системы	ПЭВМ	Windows XP Windows 7 Open Office

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине представлен в Приложении 1.

Программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденным приказом Министерства образования и науки РФ от 12 января 2016 г. № 5.

Разработал(и): _____ Урбан В.А.

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Б1.В.18. Техническая защита информации

Направление подготовки (специальность)
09.03.01 Информатика и вычислительная техника

Профиль подготовки (специализация)
“Автоматизированные системы обработки информации и управления**”**

Квалификация (степень) выпускника бакалавр

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Наименование и содержание компетенции
ОК-5 способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства

Знать:

Этап 1: Технология разработки политики ИБ АС
Этап 2: Технология разработки политики ИБ АС
Уметь:
Этап 1: Разработка политики ИБ АС
Этап 2: Умение работать с политикой ИБАС

Владеть:

Этап 1: Теоретический опыт разработки политики ИБ АС
Этап 2: Практический опыт разработки политики ИБ АС

ПК-31 способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности

Знать:

Этап 1: Технология проектирования системы управления ИБ АС
Этап 2: Технология использования системы управления ИБ АС

Уметь:
Этап 1: Проектирование системы управления ИБ АС
Этап 2: Проектирование системы управления ИБ АС

Владеть:
Этап 1: Теоретический опыт проектирования системы управления ИБ АС

Этап 2: Практический опыт проектирования системы управления ИБ АС

ПК-32 способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите

Знать:

Этап 1: Теоретические основы проведения экспериментов
Этап 2: Практические основы проведения экспериментов

Уметь:
Этап 1: Проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации
Этап 2: Проведение экспериментально-исследовательских работ при аттестации АС без учета нормативных требований по защите информации

Владеть:

Этап 1: Теоретический опыт проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации
Этап 2: Практический опыт проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации

1. Показатели и критерии оценивания компетенций на различных этапах их формирования.

Таблица 1 - Показатели и критерии оценивания компетенций на 1 этапе

Наименование компетенции	Критерии сформированности компетенции	Показатели	Способы оценки
1	2	3	4
ОК-5 способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства	владеет способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства	**Знать:** Технология разработки политики ИБ АС **Уметь:** Разработка политики ИБ АС **Владеть:** Теоретический опыт разработки политики ИБ АС	индивидуальный устный опрос, тестирование.
ПК-31 способностью	Владеет способностью	**Знать:** Технология проектирования	индивидуальный устный опрос,

разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности	разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности	системы управления ИБ АС **Уметь:** Проектирование системы управления ИБ АС **Владеть:** Теоретический опыт проектирования системы управления ИБ АС	тестирование.
ПК-32 способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	Владеет способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	**Знать:** Теоретические основы проведения экспериментов **Уметь:** Проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации **Владеть:** Теоретический опыт проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации	индивидуальный устный опрос, тестирование.

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	**Критерии сформированности компетенции**	**Показатели**	**Способы оценки**
1	2	3	4
ОК-5 способностью понимать социальную	владеет способностью понимать	**Знать:** Технология разработки политики ИБ АС	индивидуальный устный опрос, тестирование.

значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства	социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства	**Уметь:** Умение работать с политикой ИБАС **Владеть:** Практический опыт разработки политики ИБ АС	
ПК-31 способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности	Владеет способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности	**Знать:** Технология использования системы управления ИБ АС **Уметь:** Проектирование системы управления ИБ АС **Владеть:** Практический опыт проектирования системы управления ИБ АС	индивидуальный устный опрос, тестирование.
ПК-32 способностью проводить анализ особенностей деятельности организации и	Владеет способностью проводить анализ особенностей деятельности организации и	**Знать:** Практические основы проведения экспериментов **Уметь:** Проведение экспериментально-	индивидуальный устный опрос, тестирование.

использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	исследовательских работ при аттестации АС без учета нормативных требований по защите информации **Владеть:** Практический опыт проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации	

2. Шкала оценивания.

Университет использует систему оценок соответствующего государственным регламентам в сфере образования и позволяющую обеспечивать интеграцию в международное образовательное пространство. Система оценок и описание систем оценок представлены в таблицах 3 и 4.

Таблица 3 - Система оценок

Диапазон оценки, в баллах	**Экзамен**		**Зачет**
	европейская шкала (ECTS)	традиционная шкала	
[95;100]	**A** – (5+)	отлично – (5)	зачтено
[85;95)	**B** – (5)		
[70,85)	**C** – (4)	хорошо – (4)	
[60;70)	**D** – (3+)	удовлетворительно – (3)	
[50;60)	**E** – (3)		незачтено
[33,3;50)	**FX** – (2+)	неудовлетворительно – (2)	
[0;33,3)	**F** – (2)		

Таблица 4 - Описание системы оценок

ECTS	**Описание оценок**	**Традиционная шкала**
A	**Превосходно** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к	**отлично (зачтено)**

	максимальному.	
B	**Отлично** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.	
C	**Хорошо** – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено максимальным числом баллов, некоторые виды заданий выполнены с ошибками.	**хорошо (зачтено)**
D	**Удовлетворительно** – теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.	**удовлетворительно (зачтено)**
E	**Посредственно** – теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному	**удовлетворительно (незачтено)**
FX	**Условно неудовлетворительно** – теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.	**неудовлетворительно (незачтено)**
F	**Безусловно неудовлетворительно** – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные задания содержат грубые ошибки,	

	дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий.	

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

Таблица 5 **ОК-5** способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства
Этап 1

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Технология разработки политики ИБ АС	1. анализировать и оценивать угрозы информационной безопасности объекта; 2. применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
Уметь: Разработка политики ИБ АС	1. Владеть навыками работы с нормативными п- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 2. технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
Навыки: владеть Теоретический опыт разработки политики ИБ АС	1. методами и средствами выявления угроз безопасности автоматизированным системам; 2. методами технической защиты информации;

Таблица 6 - **ПК-31** способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности

Этап 1

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Технология проектирования системы управления ИБ АС	1. применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; 2. пользоваться нормативными документами по защите информации;
Уметь: Проектирование системы управления ИБ АС	1. навыками работы с нормативными п- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 2. технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
Навыки: владеть Теоретический опыт проектирования системы управления ИБ АС	1. методами и средствами выявления угроз безопасности автоматизированным системам; 2. методами технической защиты информации;

Таблица 7 - **ПК-32** способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите

Этап 1

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Теоретические основы проведения экспериментов	1. анализировать и оценивать угрозы информационной безопасности объекта; 2. применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
Уметь: Проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации	1. навыками работы с нормативными п- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 2. технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
Навыки: Теоретический опыт	1. методами формирования требований по защите информации; 2. методами расчета и инструментального контроля показателей

проведение экспериментально-исследовательских работ при аттестации АС с учетом нормативных требований по защите информации	технической защиты информации;

Таблица 8 **ОК-5** способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства
Этап 2

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Технология разработки политики ИБ АС	1. анализировать и оценивать угрозы информационной безопасности объекта; 2. применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
Уметь: Умение работать с политикой ИБАС	1. Владеть навыками работы с нормативными п- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 2. технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
Навыки: Практический опыт разработки политики ИБ АС	1. методами формирования требований по защите информации; 2. методами расчета и инструментального контроля показателей технической защиты информации;

Таблица 9 - **ПК-31** способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности

Этап 2

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Технология	1. применять отечественные и зарубежные стандарты в области

использования системы управления ИБ АС	компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; 2. пользоваться нормативными документами по защите информации;
Уметь: Проектирование системы управления ИБ АС	1. навыками работы с нормативными п- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 2. технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
Навыки: владеть Практический опыт проектирования системы управления ИБ АС	1. методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; 2. профессиональной терминологией.

Таблица 10 - **ПК-32** способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите

Этап 2

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: Практические основы проведения экспериментов	1. применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; 2. пользоваться нормативными документами по защите информации;
Уметь: Проведение экспериментально-исследовательских работ при аттестации АС без учета нормативных требований по защите информации	1. Владеть навыками работы с нормативными п- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; 2. технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
Навыки: Практический опыт проведение экспериментально-	- методами и средствами выявления угроз безопасности автоматизированным системам; - методами технической защиты информации; - методами формирования требований по защите информации;

исследовательских работ при аттестации АС с учетом нормативных требований по защите информации	- методами расчета и инструментального контроля показателей технической защиты информации; - методиками проверки защищенности объектов

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

В процессе изучения дисциплины предусмотрены следующие формы контроля: текущий, промежуточный контроль (экзамен), контроль самостоятельной работы студентов.

Текущий контроль успеваемости обучающихся осуществляется по всем видам контактной и самостоятельной работы, предусмотренным рабочей программой дисциплины. Текущий контроль успеваемости осуществляется преподавателем, ведущим аудиторные занятия.

Текущий контроль успеваемости может проводиться в следующих формах:

- устная (устный опрос, защита письменной работы, доклад по результатам самостоятельной работы и т.д.);
- письменная (письменный опрос, выполнение, расчетно-проектировочной и расчетно-графической работ и т.д.);
- тестовая (устное, письменное, компьютерное тестирование).

Результаты текущего контроля успеваемости фиксируются в журнале занятий с соблюдением требований по его ведению.

Промежуточная аттестация – это элемент образовательного процесса, призванный определить соответствие уровня и качества знаний, умений и навыков обучающихся, установленным требованиям согласно рабочей программе дисциплины. Промежуточная аттестация осуществляется по результатам текущего контроля.

Конкретный вид промежуточной аттестации по дисциплине определяется рабочим учебным планом и рабочей программой дисциплины.

Зачет, как правило, предполагает проверку усвоения учебного материала практические и семинарских занятий, выполнения лабораторных, расчетно-проектировочных и расчетно-графических работ, курсовых проектов (работ), а также проверку результатов учебной, производственной или преддипломной практик. В отдельных случаях зачеты могут устанавливаться по лекционным курсам, преимущественно описательного характера или тесно связанным с производственной практикой, или имеющим курсовые проекты и работы.

Экзамен, как правило, предполагает проверку учебных достижений обучаемы по всей программе дисциплины и преследует цель оценить полученные теоретические знания, навыки самостоятельной работы, развитие творческого мышления, умения синтезировать полученные знания и их практического применения.

5. Материалы для оценки знаний, умений, навыков и (или) опыта деятельности

Полный комплект оценочных средств для оценки знаний, умений и навыков находится у ведущего преподавателя.