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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.07.01 Методы и средства защиты компьютерной 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

Целями освоения дисциплины является:
- овладение способностью использовать основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач, способность анализировать социально значимые процессы и явления;
- способность собирать и анализировать научно-техническую информацию, учитывать современные тенденции развития и использовать достижения отечественной и зарубежной науки, техники и технологии в профессиональной деятельности;
- способность работать с информацией в глобальных компьютерных сетях.

2. Место дисциплины в структуре ООП

Дисциплина «Методы и средства защиты компьютерной информации» включена в цикл вариативную часть. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Основы теории управления» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Дисциплина	Раздел
Алгоритмические языки и программирование	Все разделы

Таблица 2.2 – Требования к постреквизитам дисциплины

Дисциплина	Раздел
Теоретические основы автоматизированного управления	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
ОПК-4 способностью участвовать в настройке и наладке программно-аппаратных комплексов	Этап 1: Описание 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
ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической	Этап 1: Технология проектирования системы управления ИБ АС	Этап 1: Проектирование системы управления ИБ АС Этап 2:	Этап 1: Теоретический опыт проектирования системы управления ИБ АС Этап 2:

культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Этап 2: Технология использования системы управления ИБ АС	Использование системы управления ИБ АС	Практический опыт проектирования системы управления ИБ АС

4. Объем дисциплины

Общая трудоемкость дисциплины «Методы и средства защиты компьютерной информации» составляет 3 ЗЕ (108 часов), их распределение по видам работ и по семестрам 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 №3	
				КР	СР
1	**2**	**3**	**4**	**5**	**6**
1	Лекции (Л)	16		16	
2	Лабораторные работы (ЛР)				
3	Практические занятия (ПЗ)	32		32	
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)		29		29
10	Подготовка к занятиям (ПкЗ)		29		29
11	Промежуточная аттестация	2		2	
12	Наименование вида промежуточной аттестации			зачет	
13	Всего	50	58	50	58

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1

Таблица 5.1. Структура дисциплины

№ п/п	Наименования модулей и модульных единиц	Семестр	Трудоемкость по видам учебной работы, час.										Кодыформируемых 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	7	8	9	10	11	12	13	14	15	16	17
1.	**Раздел 1 Предмет курса.**	**3**	**4**		**8**					**8**	**8**		ОПК-4 ОПК-5
1.1.	**Тема 1** Предмет, структура и краткое содержание курса.	3	2		4					4	4		ОПК-4 ОПК-5
1.2.	**Тема 2** Роль информационной безопасности в обеспечении национальной безопасности государства.	3	2		4					4	4		ОПК-4 ОПК-5
2.	**Раздел 2 Основные понятия и задачи криптографии**	**3**	**4**		**8**					**7**	**7**		ОПК-4 ОПК-5
2.1.	**Тема 3** Понятие информации, информационной безопасности АС.	3	2		4					3	3		ОПК-4 ОПК-5
2.2.	**Тема 4** Основные уровни защиты информации. Защита машинных носителей информации.	3	2		4					4	4		ОПК-4 ОПК-5
3.	**Раздел 3 Криптографические протоколы. Ключевая система шифра. Источники открытых текстов. Шифры замены. Шифры перестановки.**	**3**	**4**		**8**					**7**	**7**		ОПК-4 ОПК-5
3.1.	**Тема 5** Защита целостности программно-аппаратной среды. Защита от сбоев программно-аппаратной среды.	3	2		4					4	4		ОПК-4 ОПК-5
3.2.	**Тема 6** Дискреционная политика разграничения доступа. Описание модели Белла-Лападулы.	3	2		4					3	3		ОПК-4 ОПК-5
4.	**Раздел 4 Математическая модель симметричного шифра по К.Шеннону. Блочные шифры**	**3**	**4**		**8**					**7**	**7**		ОПК-4 ОПК-5
4.1.	**Тема 7**	3	2		4					4	3		ОПК-4

№ п/п	Наименования модулей и модульных единиц	Семестр	Трудоемкость по видам учебной работы, час.										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	7	8	9	10	11	12	13	14	15	16	17
	Классы защищенности АС. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.												ОПК-5
4.2.	**Тема 8** Исследование корректности реализации и методы верификации АС.	3	2		4					3	4		ОПК-4 ОПК-5
5.	**Контактная работа**	**3**	**16**		**32**							**2**	
6.	**Самостоятельная работа**	**3**								**29**	**29**		
7.	**Объем дисциплины в семестре**	**3**	**16**		**32**					**29**	**29**	**2**	
8.	**Всего по дисциплине**		**16**		**32**					**29**	**29**	**2**	

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Понятие защиты информации. Базовые свойства безопасности информации.	2
Л-2	Понятие угрозы, уязвимости, риска	2
Л-3	Идентификация и аутентификация субъектов	2
Л-4	Парольные системы идентификации и аутентификации пользователей	2
Л-5	Методы и средства обеспечения информационной безопасности	2
Л-6	Основы комплексного обеспечения информационной безопасности	2
Л-7	Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей	2
Л-8	Методология построения и анализа систем обеспечения информационной безопасности	2
Итого по дисциплине		16

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	Виды утечки информации	4
ПЗ-2	Понятие канала утечки информации, основные каналы утечки информации	4
ПЗ-3	Количественная оценка стойкости парольной защиты	4
ПЗ-4	Устройства идентификации	4
ПЗ-5	Методы и средства обеспечения информационной безопасности	4
ПЗ-6	Комплексная защита информации в компьютерных системах и сетях	4
ПЗ-7	Разработка практических рекомендаций по обеспечению безопасности информационных систем	4
ПЗ-8	Радиоэлектронные системы и устройства защиты информации	4
Итого по дисциплине		32

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

№ п.п.	Наименование темы	Наименование вопросов	Объем, академические часы
1	Предмет курса	Предмет, структура и краткое содержание курса. Роль информационной безопасности в обеспечении национальной безопасности государства	7
2	Основные понятия и задачи криптографии	Понятие информации, информационной безопасности АС. Основные уровни защиты информации. Защита машинных носителей информации	7
3	Криптографические протоколы. Ключевая система шифра. Источники открытых текстов. Шифры замены. Шифры перестановки.	Защита целостности программно-аппаратной среды. Защита от сбоев программно-аппаратной среды. Дискреционная политика разграничения доступа. Описание модели Белла-Лападулы.	8
4	Математическая модель симметричного шифра по К.Шеннону. Блочные шифры	Классы защищенности АС. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Исследование корректности реализации и методы верификации АС	7
Итого по дисциплине			29

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Основная литература, необходимая для освоения дисциплины

1. Стандарты информационной безопасности: курс лекций: учебное пособие . Галатенко В.А. ИНТУИТ • 2006 год • 264 страницы (КНИГАФОНД)

6.2. Дополнительная литература, необходимая для освоения дисциплины

1. Информационные технологии в управлении: Учебное пособие Граничин О.Н., Кияев В.И. ИНТУИТ; БИНОМ. Лаборатория знаний • 2008 год • 336 страниц

2. Обеспечение безопасности персональных данных Скрипник Д.А. ИНТУИТ • 2011 год • 122 страницы (КНИГАФОНД)

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 учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие включающее:
- методические рекомендации по самостоятельному изучению вопросов;
- методические рекомендации по подготовке к занятиям.

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

1. Microsoft Office

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

1. http://www.knigafund.ru/ - ЭБС

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

Номер ПЗ	Тема практической работы	Название специализированной лаборатории	Название оборудования	Название технических и электронных средств обучения и контроля знаний
ПЗ-1	Виды утечки информации	951 лаборатория проектирования информационных систем,953 лаборатория интеллектуальных систем	ПЭВМ (по количеству обучающихся)	*Microsoft Office*

ПЗ-2	Понятие канала утечки информации, основные каналы утечки информации	951 лаборатория проектирования информационных систем,953 лаборатория интеллектуальных систем	ПЭВМ (по количеству обучающихся)	*Microsoft Office*
ПЗ-3	Количественная оценка стойкости парольной защиты	951 лаборатория проектирования информационных систем,953 лаборатория интеллектуальных систем	ПЭВМ (по количеству обучающихся)	*Microsoft Office*
ПЗ-4	Устройства идентификации	951 лаборатория проектирования информационных систем,953 лаборатория интеллектуальных систем	ПЭВМ (по количеству обучающихся)	*Microsoft Office*
ПЗ-5	Разработка архитектуры модели безопасности информационных систем и сетей	951 лаборатория проектирования информационных систем,953 лаборатория интеллектуальных систем	ПЭВМ (по количеству обучающихся)	*Microsoft Office*
ПЗ-6	Комплексная защита информации в компьютерных системах и сетях	951 лаборатория проектирования информационных систем,953 лаборатория интеллектуальных систем	ПЭВМ (по количеству обучающихся)	*Microsoft Office*
ПЗ-7	Разработка практических рекомендаций по обеспечению безопасности информационных систем	951 лаборатория проектирования информационных систем,953 лаборатория интеллектуальных систем	ПЭВМ (по количеству обучающихся)	*Microsoft Office*
ПЗ-8	Радиоэлектронные системы и устройства защиты информации	951 лаборатория проектирования информационных систем,953 лаборатория интеллектуальных систем	ПЭВМ (по количеству обучающихся)	*Microsoft 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.ДВ.07.01 Методы и средства защиты компьютерной информации

Направление подготовки (специальность)
09.03.01 Информатика и вычислительная техника

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

Квалификация (степень) выпускника бакалавр

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

Наименование и содержание компетенции
ОПК-4 способностью участвовать в настройке и наладке программно-аппаратных комплексов
Знать:
Этап 1: Описание 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

Наименование и содержание компетенции
ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
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: Использование системы управления ИБ АС
Владеть:
Этап 1: Теоретический опыт проектирования системы управления ИБ АС
Этап 2: Практический опыт проектирования системы управления ИБ АС

2. 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
ОПК-4 способностью участвовать в настройке и наладке программно-аппаратных комплексов	способность участвовать в настройке и наладке программно-аппаратных комплексов	**Знать:** Описание политики ИБ АС. **Уметь:** Разработка политики ИБ АС. **Владеть:** Теоретический опыт разработки политики ИБ АС.	индивидуальный устный опрос, практическое решение задач, тестирование.
ОПК-5 способностью решать стандартные задачи	способность решать стандартные задачи профессиональной деятельности на	**Знать:** Технология проектирования системы управления ИБ АС.	индивидуальный устный опрос, практическое решение задач,

профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Уметь:** Проектирование системы управления ИБ АС. **Владеть:** Теоретический опыт проектирования системы управления ИБ АС.	тестирование.

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	**Критерии сформированности компетенции**	**Показатели**	**Способы оценки**
1	2	3	4
ОПК-4 способностью участвовать в настройке и наладке программно-аппаратных комплексов	способность участвовать в настройке и наладке программно-аппаратных комплексов	**Знать:** Технология разработки политики ИБ АС. **Уметь:** Умение работать с политикой ИБАС. **Владеть:** Практический опыт разработки политики ИБ АС.	индивидуальный устный опрос, практическое решение задач, тестирование.
ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** Технология использования системы управления ИБ АС. **Уметь:** Использование системы управления ИБ АС. **Владеть:** Практический опыт проектирования системы управления ИБ АС.	индивидуальный устный опрос, практическое решение задач, тестирование.

3. 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

<table>
<tr><th rowspan="2">Диапазон оценки, в баллах</th><th colspan="2">Экзамен</th><th rowspan="2">Зачет</th></tr>
<tr><th>европейская шкала (ECTS)</th><th>традиционная шкала</th></tr>
<tr><td>[95;100]</td><td>A – (5+)</td><td rowspan="2">отлично – (5)</td><td rowspan="3">зачтено</td></tr>
<tr><td>[85;95)</td><td>B – (5)</td></tr>
<tr><td>[70,85)</td><td>C – (4)</td><td>хорошо – (4)</td></tr>
<tr><td>[60;70)</td><td>D – (3+)</td><td rowspan="2">удовлетворительно – (3)</td><td rowspan="3">незачтено</td></tr>
<tr><td>[50;60)</td><td>E – (3)</td></tr>
<tr><td>[33,3;50)</td><td>FX – (2+)</td><td rowspan="2">неудовлетворительно – (2)</td></tr>
<tr><td>[0;33,3)</td><td>F – (2)</td></tr>
</table>

Таблица 4 - Описание системы оценок

<table>
<tr><th>ECTS</th><th>Описание оценок</th><th>Традиционная шкала</th></tr>
<tr><td>A</td><td>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 максимальному.</td><td rowspan="2">отлично (зачтено)</td></tr>
<tr><td>B</td><td>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.</td></tr>
<tr><td>C</td><td>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.</td><td>хорошо (зачтено)</td></tr>
</table>

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.	

4. 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 - ОПК-4 способностью участвовать в настройке и наладке программно-аппаратных комплексов. 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: Описание политики ИБ АС.	1. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами 2. Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES 3. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.
Уметь: Разработка политики ИБ АС.	4. Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в режимах гаммирования. 5. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра Решетка ценности. 6. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.
Навыки: Теоретический опыт разработки политики ИБ АС.	7. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма Защита машинных носителей информации 8. Электронная подпись. Варианты электронной подписи на основе алгоритмов RSA и Эль-Гамаля. Основные виды атак на информационные АС 9. Хэш-функции и их применение. Хеш-функция MD2.

Таблица 6 - ОПК-4 способностью участвовать в настройке и наладке программно-аппаратных комплексов. 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. Однонаправленные (односторонние) функции с секретом и их применение. 2. Криптографические методы защиты. 3. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
Уметь: Умение работать с политикой	4. Защита целостности программно-аппаратной среды. 5. Основные методы защиты памяти

ИБАС.	6. Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамаля
Навыки: Практический опыт разработки политики ИБ АС.	7. Эксплуатационно-технологические меры защиты. 8. Понятие политики безопасности 9. Дискреционная политика разграничения доступа

Таблица 7 - ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. 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. Понятие и роль информации в жизни современного общества. 2. Информационные революции в истории человечества и их характеристика. 3. Виды информации. 4. Информационные технологии и их юридическая характеристика. 5. Информационные ресурсы и их юридическая характеристика.
Уметь: Проектирование системы управления ИБ АС.	6. Деятельность государства в информационной сфере. 7. Понятие и признаки информационного общества, место в нем современной России. 8. Понятие, предмет и методология отечественного информационного права. 9. Информационное право Российской Федерации как отрасль права, его соотношение со смежными отраслями права. 10. Основные понятия и категории информационного права.
Навыки: Теоретический опыт проектирования системы управления ИБ АС.	11. Система источников информационного права. 12. Роль и место международных источников права в системе отечественного информационного права. 13. Окинавская хартия глобального информационного общества (принята 22 июля 2000 г. лидерами стран «Большой Восьмерки», Окинава, Япония). 14. Роль и место Конституции России в системе источников информационного права Российской Федерации. 15. Роль и место гражданского законодательства Российской Федерации в системе источников информационного права.

Таблица 8 - ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. 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 использования системы управления ИБ АС.	1.Перехват данных является угрозой: а)доступности +б)конфиденциальности в)целостности 2.Что из перечисленного не относится к числу основных аспектов информационной безопасности: а)доступность б)целостность +в)защита от копирования г)конфиденциальность 3.В число целей политики безопасности верхнего уровня входят: +а)формулировка административных решений по важнейшим аспектам б)реализации программы безопасности в)выбор методов аутентификации пользователей +г)обеспечение базы для соблюдения законов и правил 4.В число граней, позволяющих структурировать средства достижения информационной безопасности, входят: +а)законодательные меры б)меры обеспечения доступности в)профилактические меры 5.Оценка рисков позволяет ответить на следующие вопросы: +а)существующие риски приемлемы? б)кто виноват в том, что риски неприемлемы? +в)что делать, чтобы риски стали приемлемыми?
Уметь: Использование системы управления ИБ АС.	6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? +А) Поддержка высшего руководства Б) Эффективные защитные меры и методы их внедрения С) Актуальные и адекватные политики и процедуры безопасности Г) Проведение тренингов по безопасности для всех сотрудников 7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б) Когда риски не могут быть приняты во внимание по политическим соображениям С) Когда необходимые защитные меры слишком сложны +Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери 8. Что такое политики безопасности? А) Пошаговые инструкции по выполнению задач безопасности Б) Общие руководящие требования по достижению определенного

	уровня безопасности +С) Широкие, высокоуровневые заявления руководства Г) Детализированные документы по обработке инцидентов безопасности 9. Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство +в) Владелец г) Пользователь 10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? +а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)
Навыки: Практический опыт проектирования системы управления ИБ АС.	11.В число этапов управления рисками входят: +а)анализ угроз б)угрозы проведения анализа +в)выявление уязвимых мест 12.Агрессивное потребление ресурсов является угрозой: +а)доступности б)конфиденциальности в)целостности 13.В рамках программы безопасности нижнего уровня определяются: а)совокупность целей безопасности +б)набор используемых механизмов безопасности в)наиболее вероятные угрозы безопасности 14."Общие критерии" содержат следующие виды требований: +а)функциональные +б)доверия безопасности в)экономической целесообразности 15.В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на: а)системы электронной коммерции б)инфраструктуру для электронных цифровых подписей +в)средства электронной аутентификации

5. 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 (зачет и 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 обучаемых 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.

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

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