

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07 КОИБАС

Направление подготовки 10.03.01 Информационная безопасность

Профиль подготовки Безопасность автоматизированных систем

Квалификация выпускника бакалавр

Форма обучения очная

1. Цели освоения дисциплины

Целью освоения дисциплины «КОИБАС» является

- подготовка к разработке системы управления информационной безопасностью автоматизированных систем, администрирование подсистем информационной безопасности автоматизированных систем.

2. Место дисциплины в структуре образовательной программы

Дисциплина «КОИБАС» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «КОИБАС» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ПК-6	Техническая защита информации
ПК-6	Метрология, стандартизация и сертификация
ПК-8	Программно-аппаратные средства защиты информации
ПК-8	Русский язык и культура речи
ПК-8	Психология и педагогика
ПК-8	Инженерная графика
ПК-8	Компьютерная графика
ПК-13	Маркетинг
ПК-15	Организационное и правовое обеспечение информационной безопасности
ПК-15	Теоретические основы защиты информации
ПК-15	Стандарты информационной безопасности

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4	Производственная эксплуатационная практика
ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4	Производственная (преддипломная) практика
ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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
ПК-6- способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Этап 1: общие методологические принципы построения комплексных систем обеспечения информационной безопасности;	Этап 1: проводить работы на автоматизированных системах специального назначения	Этап 1: основами инструментальным и с специального назначения
ПК-6- способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Этап 2: комплекс мероприятий по обеспечению информационной безопасности автоматизированных систем	Этап 2: осуществлять установку, настройку и техническое сопровождение программного обеспечения	Этап 2: навыками оценки эффективности функционирования систем управления специального назначения
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Этап 1: рабочую техническую документацию	Этап 1: применять комплексные подходы к решению задач информационной безопасности	Этап 1: методами работы с нормативно-правовыми актами

ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Этап 2: нормативные и методические документы	Этап 2: анализировать задачи информационной безопасности	Этап 2: навыками работы с нормативно-правовыми актами
ПК-13- способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Этап 1: методы проектирования систем обеспечения информационной безопасности	Этап 1: использовать современные способы борьбы с несанкционированным доступом информации	Этап 1: средствами обнаружения, блокирования вторжений.
ПК-13- способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Этап 2: средства проектирования систем обеспечения информационной безопасности	Этап 2: использовать методы копирования, изменения и сбора информации	Этап 2: современными средствами и системами сбора и защиты информации

<p>ПК-15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами</p>	<p>Этап 1: нормативные документы, регламентирующие работу ФСТЭК</p>	<p>Этап 1: проводить работы на автоматизированных системах специального назначения</p>	<p>Этап 1: основами инструментальным и с специального назначения</p>
<p>ПК-15 - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами</p>	<p>Этап 2: нормативные документы, регламентирующие работу ФСБ</p>	<p>Этап 2: осуществлять установку, настройку и техническое сопровождение программного обеспечения</p>	<p>Этап 2: навыками оценки эффективности функционирования систем управления специального назначения</p>
<p>ПСК-4.3 – Способен планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации</p>	<p>Этап 1: методы оценки качества систем</p>	<p>Этап 1: планировать комплекс мероприятий по защите информации</p>	<p>Этап 1: первичными навыками работы с основными средствами обеспечения информационной безопасности.</p>

ПСК-4.3 – Способен планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	Этап 2: модели комплексной системы информационной безопасности	Этап 2: организовывать надежность защиты аппаратных и программных средств обработки информации	Этап 2: практическим опытом работы с основными средствами обеспечения информационной безопасности
ПСК-4.4 – Способен участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Этап 1: программные и аппаратные средства АС	Этап 1: использовать современные способы борьбы с несанкционированным доступом информации	Этап 1: средствами обнаружения, блокирования вторжений.
ПСК-4.4 – Способен участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Этап 2: методику аттестации средств объектов информатизации	Этап 2: использовать методы копирования, изменения и сбора информации.	Этап 2: современными средствами и системами сбора и защиты информации

4. Объем дисциплины

Объем дисциплины «КОИБАС» составляет 4 зачетных единицы (144 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 №8	
				КР	СР
1	2	3	4	5	6
1	Лекции (Л)	26		26	
2	Лабораторные работы (ЛР)				
3	Практические занятия (ПЗ)	24		24	
4	Семинары(С)				
5	Курсовое проектирование (КП)	2		2	
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)		30		30
10	Подготовка к занятиям (ПкЗ)		60		60
11	Промежуточная аттестация	54		2	
12	Наименование вида промежуточной аттестации	х	х	зачет	
13	Всего	54	90	54	90

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 Угрозы ИБ.	8	8		8					10	20	x	ПК-6; ПК-8; ПК-13; ПК-15 ПСК-4.3; ПСК-4.4;
1.1.	Тема 1 Классификация угроз ИБ .	8	2		2			x			4	x	ПК-6; ПК-8; ПК-13; ПК-15;
	Тема 2 Анализ угроз ИБ.	8	2		2			x				x	ПК-6; ПК-8; ПК-13; ПК-15;
	Тема 3 Технические каналы утечки информации	8	2		2			x			4	x	ПК-6; ПК-8; ПК-13; ПК-15;
	Тема 4 Акустические каналы утечки		2		2			x				x	ПК-6; ПК-8; ПК-13;

№ 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
	информации.	8											ПК-15; ПСК-4.3; ПСК-4.4
	Тема 5 ПЭМИН.	8						x		4	4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 6 Закладные устройства.	8						x		2		x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 7 Визуально-оптические каналы утечки информации.	8						x		2	4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 8 Материально-вещественные каналы утечки информации.	8						x		2	4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3;

№ 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
													ПСК-4.4
2.	Раздел 2 Постановка проблемы КОИБАС.	8	8		8			x		10	20	x	ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
2.1.	Тема 9 Методология построения КОИБАС.	8	2		2			x			4	x	ПК-6; ПК-8; ПК-15; ПСК-4.3; ПСК-4.4
2.2.	Тема 10 Определение состава компонентов КСИБ.	8	2		2			x				x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 11 Стадии и этапы проектирования КСИБ.	8	2		2			x			4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 12 Формирование задач защиты информации.	8	2		2			x			4	x	ПК-6; ПК-8; ПК-13; ПСК-4.3;

№ 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
													ПСК-4.4
	Тема 13 Функциональные и обеспечивающие подсистемы КСИБ.	8						x		4		x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 14 Правовые аспекты защиты информации.	8						x		2	4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 15 Организационные мероприятия по защите информации.	8						x		2	4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 16 Инженерно-технические мероприятия по ЗИ.	8						x		2		x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
8.	Раздел 3		10		8			x		10	20	x	ПК-6;

№ 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
	Оценка качества КСИБ.	8											ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
8.1.	Тема 17 Политика информационной безопасности.	8	2		1			x			4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
8.2.	Тема 18 Модель нарушителя.	8	2		1			x			4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 19 Классификация защищенности АС.	8	2		2			x				x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 20 Оценка защищенности АС.	8	2		2			x			4	x	ПК-6; ПК-8; ПК-13;

№ 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
													ПК-15; ПСК-4.3; ПСК-4.4
	Тема 21 Аттестация объектов защиты.	8	2		2			x			4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 22 Эксплуатационная документация КСИБ	8						x		2		x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 23 Оценка технико-экономического уровня и эффективности КСИБ.	8						x		2	4	x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 24 Управление деятельностью организации по КОИБАС.	8						x		2		x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3;

№ 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
													ПСК-4.4
	Тема 25 Перспективы развития элементов КОИБАС.	8						x		2		x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
	Тема 26 Натурные испытания КС защиты.	8						x		2		x	ПК-6; ПК-8; ПК-13; ПК-15; ПСК-4.3; ПСК-4.4
12.	Контактная работа	x	26		24		2	x				2	x
12.	Самостоятельная работа	x						x		30	60		x
14.	Объем дисциплины в семестре	x	26		24		2	x		30	60	2	x
15.	Всего по дисциплине	x	26		24		2	x		30	60	2	x

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Классификация угроз ИБ .	2
Л-2	Анализ угроз ИБ.	2
Л-3	Технические каналы утечки информации	2
Л-4	Акустические каналы утечки информации	2
Л-5	Методология построения КОИБАС	2
Л-6	Определение состава компонентов КСИБ	2
Л-7	Стадии и этапы проектирования КСИБ	2
Л-8	Формирование задач защиты информации	2
Л-9	Политика информационной безопасности	2
Л-10	Модель нарушителя	2
Л-11	Классификация защищенности АС	2
Л-12	Оценка защищенности АС	2
Л-13	Аттестация объектов защиты	2
Итого по дисциплине		26

5.2.2 – Темы практических занятий

№ п.п.	Наименование темы практических занятий	Объем, академические часы
ПЗ-1	Классификация угроз ИБ .	2
ПЗ-2	Анализ угроз ИБ.	2
ПЗ-3	Технические каналы утечки информации	2
ПЗ-4	Акустические каналы утечки информации	2
ПЗ-5	Методология построения КОИБАС	2
ПЗ-6	Определение состава компонентов КСИБ	2
ПЗ-7	Стадии и этапы проектирования КСИБ	2
ПЗ-8	Формирование задач защиты информации	2
ПЗ-9	Политика информационной безопасности	1
ПЗ-10	Модель нарушителя	1
ПЗ-11	Классификация защищенности АС	2

ПЗ-12	Оценка защищенности АС	2
ПЗ-13	Аттестация объектов защиты	2
Итого по дисциплине		24

5.2.3 Темы курсовых работ (проектов)

В процессе изучения дисциплины в 8 семестре обучения студенты должны выполнить курсовой проект.

Курсовой проект выполняется с целью:

- расширения знаний по определенному разделу дисциплины КОИБАС :
- систематизации знаний по смежным дисциплинам;
- выработки у студента навыков научно-исследовательской работы;
- обучения студентов методам аналитической и проектной работы в области построения КСИБ.

Тематика курсовых проектов

1. Защита информации, как мера выживаемости организации.
2. Решение современных проблем информационной безопасности корпоративных вычислительных сетей.
3. Назначение и характер аппаратных средств защиты информации .
4. Организация безопасной корпоративной компьютерной сети в предприятии .
5. Защита информации: цифровая подпись.
6. Системы обнаружения атак. (Анализаторы сетевых протоколов и сетевые мониторы) .
7. Защита баз данных .
8. Анализ криптостойкости методов защиты информации в операционных системах Microsoft Window .
9. Парольные методы защиты информации в компьютерных системах от несанкционированного доступа.
10. Комплекс технических решений по защите информации, записанной на отчуждаемых электронных носителях от несанкционированного копирования и распространения.
11. Защита почтовых сообщений.
12. Международные стандарты для построения системы информационной безопасности.
13. Экспертно-статистический подход к оценке информационной безопасности АС.
14. Современные модели и методы оценки безопасности информации.
15. Безопасность работы в сети Интернет.
16. Безопасность в распределенных системах.
17. Инструментарий несанкционированного доступа.
18. Криптографические методы защиты информации. Метод комбинированного шифрования.
19. Безопасность файловых ресурсов сети Windows.
20. Информационная безопасность в бизнесе.
21. Повышение информационной безопасности предприятия.
22. Нормативное регулирование функционирования рынка программного обеспечения .
23. Угрозы конфиденциальной информации.
24. Средства контроля эффективности защиты информации.
25. Контроль организации защиты информации .
26. Показатели эффективности защиты информации.
27. Методы определения границ охраняемой зоны (территории).

28. Выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников.
29. Технические средства пассивной защиты информации.
30. Организационно-технические мероприятия по защите информации.
31. Планирование комплексной системы защиты информации.
32. Технические мероприятия по защите конфиденциальной информации.
33. Методы обеспечения информационной безопасности предприятия.
34. Разработка методов и средств мониторинга для выявления фактов применения несанкционированных информационных воздействий.
35. Разработка методологии и методического аппарата оценки ущерба от воздействия угроз информационной безопасности.
36. Определение критериев уязвимости и устойчивости систем к деструктивным воздействиям
37. Модель и программа оценки систем защиты.
38. Внедрение аппаратной аутентификации защиты на предприятии.
39. Аудит информационной безопасности банка.
40. Система управления информационной безопасностью "Матрица" .
41. Проблемы безопасности и надежности в информационных сетях.
42. Аппаратно-программные средства информационной безопасности.
43. Формирование функции информационной безопасности.
44. Подготовка технического задания к КСИБ.
45. Методика выявления каналов НСД и ПЭМИН.
46. Структура системы защиты информации АС.
47. Выделение ядра и ресурсов системы защиты информации.
48. Подбор средств для КСИБ.
49. Разработка наполнения и документации к КСИБ.
50. Оценка качества разработанной КСИБ
51. Целевая функция информационной безопасности.
52. Разработка методики оценки качества КСИБ.
53. Моделирование процессов утечки информации.

5.2.4 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	ПЭМИН	1. Формальная модель злоумышленника. 2. Неформальная модель злоумышленника.	4
2.	Закладные устройства	1. Принципы и подходы построения КОИБАС. 2. Требования к концепции комплексной защиты информации	2
3.	Визуально-оптические каналы утечки информации	1. Перечень полноты множества функций защиты. 2. Источники угроз информационной безопасности объекта.	2
4.	Материально-вещественные каналы утечки информации	1. Модель построения системы информационной безопасности предприятия. 2. безопасности предприятия.	2
5.	Функциональные и обеспечивающие подсистемы КСИБ	1. Этапы проектирования Комплексной системы обеспечения информационной безопасности. 2. Типовая структура Комплексной системы обеспечения информационной безопасности.	4
6.	Правовые аспекты защиты информации	1. Предпроектное исследование системы безопасности. 2. Организационный элемент КСИБ.	2
7	Организационные мероприятия по защите информации	1. Правовой элемент КСИБ.	2

		2. Инженерно-технический элемент КСИБ.	
8.	Инженерно-технические мероприятия по ЗИ	1. Программно-аппаратный элемент КСИБ. 2. Криптографический элемент КСИБ.	2
9.	Эксплуатационная документация КСИБ	1. Организационно-распорядительная составляющая КСИБ. Комплекс внутренних документов. 2. Подсистемы технической составляющей КСИБ.	2
10.	Оценка технико-экономического уровня и эффективности КСИБ.	1. Назначение и состав подсистемы обнаружения атак. 2. Назначение и состав подсистемы управления информационной безопасностью, централизованного мониторинга и аудита событий.	2
11.	Управление деятельностью организации по КОИБАС	1. Назначение и состав подсистемы идентификации и аутентификации пользователей. 2. Требования к подсистеме регистрации и учета.	2
12.	Перспективы развития элементов КОИБАС	1. Требования, предъявляемые к подсистеме обеспечения целостности. 2. Средства обнаружения утечки информации по радиоканалам.	2
13.	Натурные испытания КС защиты	1. Подготовка помещений к проведению	2

		конфиденциальных совещаний. 2. ПЭМИН . Средства поиска ПЭМИН.	
Итого по дисциплине			30

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Мельников В.П. Информационная безопасность и защита информации. Учебное пособие. Под редакцией С.А. Клейменова.-3-е изд., М.: Издательский центр «Академия» , 2008 - 336 с.

2. Расторгуев С.П. Основы информационной безопасности. Учебное пособие-М.:Изд-кий центр «Академия»,2007.-192с.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Организационная защита информации: учебное пособие для вузов
Авторы: Аверченков В.И., Рытов М.Ю. Издательство: ФЛИНТА, 2011 г.

2. Правоведение: учебникАвтор: Мухаев Р.Т. Издательство: Юнити-Дана, 2011 г.

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 (семинарских) 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;
- методические рекомендации по выполнению курсовой работы (проекта).

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

1. Microsoft Windows XP
2. Open Office
3. Google Chrome
4. Ubuntu

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

1. <http://fstec.ru/normotvorcheskaya/akty>
2. <http://ivo.garant.ru/#/basesearch>
3. http://www.consultant.ru/document/cons_doc_LAW_61798/

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

Вид и номер занятия	Тема занятия	Название специализированной аудитории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
ПЗ-1	Классификация угроз ИБ	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-2	Анализ угроз ИБ	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-3	Технические каналы утечки информации	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-4	Акустические каналы утечки информации	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-5	Методология построения КОИБАС	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-6	Определение состава компонентов КСИБ	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-7	Стадии и этапы проектирования КСИБ	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор

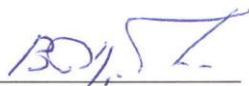
ПЗ-8	Формирование задач защиты информации	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-9	Политика информационной безопасности	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-10	Модель нарушителя	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-11	Классификация защищенности АС	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-12	Оценка защищенности АС	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор
ПЗ-13	Аттестация объектов защиты	943 «Лаборатория технологий, методов программирования и программного обеспечения»	ПЭВМ (по количеству обучающихся)	Мультимедийный проектор

Практические занятия проводятся в аудиториях, оборудованных учебной доской, рабочим местом преподавателя (стол, стул), а также посадочными местами для обучающихся, число которых соответствует численности обучающихся в группе.

Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Министерства образования и науки РФ № 1515 от 01.12.2016 г.

Разработал(и): _____



Урбан В.А.

