

АННОТАЦИЯ ДИСЦИПЛИНЫ

«Комплексное обеспечение защиты информации объекта информатизации»

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации» является частью программы бакалавриата «Информационная безопасность (общий профиль, СУОС)» по направлению «10.03.01 Информационная безопасность».

Цели и задачи дисциплины

Сформировать компетентности в области разработки комплексной системы защиты информации объекта информатизации, на основе оценки угроз безопасности информации, способов моделирования, технологии организации, кадрового, технологического и нормативно-методического обеспечения, методах оценки эффективности подобных систем. Задачи дисциплины: 1.изучение сущности, целей и задач комплексной системы защиты информации; 2.изучение принципов и этапов разработки комплексной системы защиты информации; 3.освоение технологии установления состава защищаемой информации и объектов защиты информации на объекте информатизации; 4.овладение методами оценки угроз безопасности информации; 5.изучение параметров и структуры комплексной системы защиты информации; 6.установление состава мероприятий по обеспечению функционирования комплексной системы защиты информации; 7.изучение показателей и методик эффективности системы защиты информации.

Изучаемые объекты дисциплины

Предметом освоения дисциплины являются следующие объекты: система защиты информации; анализ и оценки угроз защищаемой информации; модель процессов защиты информации; технологическое и организационное построение системы защиты информации; кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации на объекте информатизации; планирование и контроль комплексной системы защиты информации на предприятии; эффективность системы защиты информации; аттестации объектов информатизации по требованиям безопасности информации..

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		7	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	54	54	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	24	24	
- лабораторные работы (ЛР)			
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	28	28	
- контроль самостоятельной работы (КСР)	2	2	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	54	54	
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	144	144	

Краткое содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
7-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Концептуальные основы разработки комплексной системы защиты информации и определения объектов защиты	8	0	8	18
<p>Тема 1. Введение в дисциплину. Сущность комплексной системы защиты информации и принципы ее организации. Цель, задачи дисциплины, значение ее для подготовки специалиста. Знания и умения студентов, которые должны быть получены в результате ее изучения. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности объекта информатизации. Принципы организации комплексной системы защиты информации.</p> <p>Тема 2. Методологические и концептуальные основы комплексной системы защиты информации. Методология защиты информации и ее основные задачи. Уровень обеспечения безопасности информации. Достаточность защиты информации. Варианты построения комплексной системы защиты. Основные факторы, влияющие на организацию комплексной системы защиты информации. Характер и степень влияния различных факторов на организацию системы защиты информации.</p> <p>Тема 3. Определение и нормативное закрепление информации ограниченного доступа. Классификация информации по видам тайны и степеням конфиденциальности. Этапы работы по выявлению состава защищаемой информации. Нормативное закрепление состава защищаемой информации. Порядок организации нормативного закрепления информации ограниченного доступа.</p> <p>Тема 4. Определение состава объектов защиты. Понятие объекта защиты. Последовательность определения объекта защиты. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации. Методика выявления состава носителей защищаемой информации. Основные и вспомогательные</p>				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
технические средства и системы. Особенности помещений как объектов защиты.				
Особенности построения комплексной системы защиты информации объекта информатизации и оценка ее эффективности	10	0	12	18
<p>Тема 8. Технологическое и организационное построение комплексной системы защиты информации. Общее содержание работ по организации комплексной системы защиты информации. Характеристика технологического и организационного направлений создания комплексной системы защиты информации. Содержание стадий построения комплексной системы защиты информации. Предпроектное обследование. Назначение и структура техниче-ского задания, технико-экономического обоснования. Технический проект, рабочий проект. Аprobация системы защиты информации и ввод ее в эксплуатацию.</p> <p>Тема 9. Кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации. Кадровое обеспечение функционирования комплексной системы защиты информации. Защита человеческих ресурсов. Распределение функций по защите информации. Материально-техническое обеспечение защиты информации. Нормативно-методическое обеспечение комплексной защиты информации на предприятии. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.</p> <p>Тема 10. Планирование и контроль комплексной системы защиты информации. Понятие, принципы и методы планирования комплексной системы защиты информации. Стадии планирования. Факторы, влияющие на выбор принципов и способов планирования. Структура и общее содержание планов предприятия и функционирования комплексной системы защиты информации. Организация выполнения планов. Сущность, цель, задачи и содержание контроля комплексной системы защиты информации. Виды и методы</p>				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
<p>контроля системы защиты информации. Основные контрольные мероприятия по защите информации.</p> <p>Тема 11. Оценка эффективности комплексной системы защиты информации. Понятие эффективности и эффективности защиты информации. Требование по защите информации. Показатель и норма эффективности защиты информации. Подходы к оценке эффективности систем защиты информации и их особенности. Состав методов и моделей оценки эффективности систем защиты информации. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.</p> <p>Тема 12. Аттестация объектов информатизации по требованиям безопасности информации. Состав и содержание нормативно - правовых актов по аттестации объектов информатизации. Система аттестации объектов информатизации по требованиям безопасности информации. Организация аттестационных испытаний. Типовое содержание аттестационных испытаний объектов информатизации. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа</p> <p>Аттестационные испытания объектов вычислительной техники по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок. Аттестационные испытания выделенных помещений. Инструментальные средства для проведения аттестационных испытаний. Основы проведения поисковых мероприятий по выявлению закладочных устройств.</p>				
<p>Моделирование угроз безопасности информации и процессов защиты информации на объекте информатизации</p>	6	0	8	18
<p>Тема 5. Источники, способы и результаты дестабилизирующего воздействия на</p>				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
<p>информацию. Определение источников дестабилизирующего воздействия на информацию.</p> <p>Модель формирования множества дестабилизирующих факторов. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации.</p> <p>Классификация угроз безопасности информации для объекта информатизации.</p> <p>Анализ и оценка угроз информационной безопасности объекта.</p> <p>Тема 6. Выявление каналов утечки и методов несанкционированного воздействия на информацию. Сущность утечки информации и несанкционированного воздействия на информацию. Структурная модель канала утечки информации. Технические каналы утечки информации и их классификация. Модель технических каналов утечки информатизации на типовом объекте информатизации. Каналы утечки из-за несанкционированного воздействия на информацию на системы, использующие информационно - коммуникационные технологии. Инсайдерские каналы утечки информации и «социальный инжиниринг» Методы «социального инжиниринга».</p> <p>Тема 7. Моделирование процессов защиты информации. Понятие модели и объекта моделирования. Основные виды моделей и их характеристика. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации. Понятие архитектуры системы защиты информации. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации. Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.</p>				
ИТОГО по 7-му семестру	24	0	28	54
ИТОГО по дисциплине	24	0	28	54