АННОТАЦИЯ ДИСЦИПЛИНЫ

«Основы информационной безопасности »

Дисциплина «Основы информационной безопасности » является частью программы специалитета «Безопасность открытых информационных систем (СУОС)» по направлению «10.05.03 Информационная безопасность автоматизированных систем».

Цели и задачи дисциплины

Цель - изучение принципов обеспечения информационной безопасности и защиты информации, подходов к анализу угроз безопасности информационных систем и освоение компетенций для решения основных задач защиты информации в информационных системах Задачи дисциплины: - изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации; - изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн; - изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем; - приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации; - приобретение навыков анализа информационной инфраструктуры с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации..

Изучаемые объекты дисциплины

основные понятия, общеметодологические принципы теории информационной безопасности; - основы государственной информационной политики по обеспечению безопасности информации; - виды информации ограниченного доступа; - угрозы безопасности информации и уязвимости информационных систем; - информационные войны и информационное оружие; - методы нарушения конфиденциальности, целостности и доступности информации; - причины, виды каналы утечки информации и несанкционированного доступа; - формальные модели безопасности информации; - уровни и сервисы защиты информации; - способы и средства защиты информации; - критерии оценки защищенности информационных систем; - основы организации защиты информации на предприятии..

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		2
1. Проведение учебных занятий (включая проведе-ние текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	24	24
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	27	27
- контроль самостоятельной работы (КСР)	3	3
- 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
2-й семестр				
Понятие и виды угроз информационной безопасности	2	0	2	4
Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Уровни и сервисы защиты информации в информационных системах	2	0	2	4
Единые критерии безопасности информационных технологий. Законодательный, административный, процедурный уровни информационной безопасности. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.				
Информационная безопасность и информационное противоборство	2	0	2	4
Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Информационная война как способ воздействия на информационные системы различного назначения и объекты критической информационной инфраструктуры				
Основные понятия и общеметодологические принципы теории информационной безопасности	2	0	2	4
Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности.				
Формальные модели безопасности автоматизированных систем	2	0	2	6
Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом.				
Понятие и виды защищаемой информации.	2	0	2	4
Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты.				
Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	2	0	2	4
Основные составляющие национальных интересов Российской Федерации в ин-формационной сфере. Информационная безопасность Российской Федерации. Интересы личности в информационной сфере. Интересы общества в инфор¬мационной сфере. Интересы государства в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.				
Защита информации от технических разведок	2	0	2	4
Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированных систем. Понятие и классификация видов технических разведок. Классификация технических каналов утечки информации. Способы и				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
средства защиты информации от утечки по техническим каналам.				
Защита информации криптографическими методами	2	0	2	6
Понятие криптографической защиты информации. Системы Шеннона. Типы и свойства шифров. Симметричные и асимметричные криптосистемы. Преобразование по схеме Фейстеля. Шифр DES, ГОСТ 28147-89. Алгоритм шифрования RSA.Управление криптографическими ключами. Протокол Kerberos. Криптографическая система Эль-Гамаля. Понятие Хэш-функции. Инфраструктура открытых ключей (PKI). Средства криптографической защиты информации и электронной подписи. Криптографические средства защиты информации.				
Способы и средства защиты информации	2	0	4	4
Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности, DLP, SIEM-системы. Комплексные решения в обеспечении защиты информации, SOC-центры.				
Основы безопасности сетевых технологий	2	0	3	4
Базовая эталонная модель взаимодействия открытых систем (OSI). Уровни и основные протоколы сетевого взаимодействия. Концепция сетевых зон. Протокол IPsec. VPN. Типы брандмауэров и принципы фильтрации трафика. Системы обнаружения/предотвращения вторжений (IDS/IPS). Защита Web-приложений.				
Критерии оценки защищенности информационных систем	2	0	2	6
Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
систем. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий. Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000.				
ИТОГО по 2-му семестру	24	0	27	54
ИТОГО по дисциплине	24	0	27	54