

АННОТАЦИЯ ДИСЦИПЛИНЫ

«Безопасность операционных систем»

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

Цели и задачи дисциплины

освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе реализации требований по правовой защите информации и организационному обеспечению информационной безопасности..

Изучаемые объекты дисциплины

ознакомление с политикой безопасности компании в области информационной безопасности; ознакомление со стандартами информационной безопасности; изучение криптографических методов и алгоритмов шифрования информации; изучение алгоритмов аутентификации пользователей; приобретение навыков защиты информации в сетях; изучение требований к системам защиты информации. приобретение умений в разработке проектов нормативных и организационно-распорядительных документов в области обеспечения информационной безопасности и их применении; приобретение навыков работы в организации и обеспечении режима секретности, физической защиты объектов, методах организации работы с персоналом и управлению деятельностью служб защиты информации на предприятии..

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		9	10
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	144	72	72
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	72	36	36
- лабораторные работы (ЛР)	32	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	36	18	18
- контроль самостоятельной работы (КСР)	4	2	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	180	108	72
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет	9		9
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)	18	18	
Общая трудоемкость дисциплины	360	216	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
9-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
Методы обеспечения безопасности информационных систем	18	16	10	54
Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Организация информационной безопасности компании. Выбор средств информационной информации. Информационное страхование				
Безопасность информационных систем	18	0	8	54
Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Международные стандарты информационного обмена. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Виды угроз информационной безопасности. Три вида возможных нарушений информационной системы. Защита. Источники угроз информационной безопасности РФ. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
противников или «нарушителей». Удаленные атаки на интрасети Стандарты безопасности. Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии				
ИТОГО по 9-му семестру	36	16	18	108
10-й семестр				
Программные методы обеспечение информационной безопасности	18	8	8	36
Архитектура операционных систем. Процесс загрузки операционных систем. Классификация программного обеспечения. Защищенный режим работы процессора. Уровни доступа. Разграничение адресного пространства и ресурсов ПК. Драйверы. Сервисы. Утилиты Методы криптографии. Классификация криптографических методов. Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись. Программные интерфейсы Crypto API Условия существования вредоносных программ. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Rootkit. Спам. Защита от компьютерных вирусов. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы				
Принципы разработки защищенного программного обеспечения	18	8	10	36
Виды угроз. Разграничение доступа к ресурсам ИС. Идентификация и аутентификация пользователей в ОС семейства Windows и Linux. Аудит событий безопасности. Администрирование прав пользователей. Аппаратно-программные комплексы обеспечения безопасности ОС Управление доступом к ресурсам в программном коде. Получение информации об идентификации и аутентификации пользователей в ОС семейства Windows и Linux. Использование встроенных API шифрования Crypto API. Исследование программного кода для работы с				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
электронными ключами				
ИТОГО по 10-му семестру	36	16	18	72
ИТОГО по дисциплине	72	32	36	180