АННОТАЦИЯ ДИСЦИПЛИНЫ

«Безопасность вычислительных сетей»

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

Цели и задачи дисциплины

Цель дисциплины – формирование у студентов компетентности в области информационной безопасности вычислительных сетей. Задачи дисциплины: - изучение базовой инфраструктуры инфокоммуникационных сетей, основных устройств и систем, требований к обеспечению информационной безопасности, соответствующих стандартов, технических спецификаций, протоколов и технологий; - формирование умений по созданию, настройке и эксплуатации безопасных вычислительных сетей - овладение навыками по использованию компонентов защищенных вычислительных сетей, способностью разрабатывать модели угроз и модели нарушителей ИБ на основе исходных данных о сети.

Изучаемые объекты дисциплины

- принципы построения защищенных компьютерных телекоммуникационных сетей; - методы и проблемы оценивания угроз безопасности, угрозы безопасности, стандарты информационной безопасности; - классификация типовых угроз информационной безопасности для вычислительных сетей; - требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования; - модели и теоремы безопасности на основе дискреционной политики, модели и теоремы безопасности на основе мандатной политики; - скрытые каналы утечки информации, модели и механизмы обеспечения целостности данных; - нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты; - типовые аппаратные и программные средства обеспечения информационной безопасности вычислительных сетей..

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		9	10
1. Проведение учебных занятий (включая проведе-ние текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	144	72	72
- 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				
Политика и модели безопасности в компьютерных системах	10	4	4	24
Понятие политики безопасности. Модель безопасности как формализо-ванное выражение политики безопасности. Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС. Составляющие модели безопасности — модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС. Класс моделей конечных состояний				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Основные понятия о надежности систем ЗКТС	8	4	4	22
Основы теории надежности систем связи. Факторы, влияющие на надежность защищенных телекоммуникационных систем; модели надежности; оценка показателей надежности; методы обеспечения надежности; влияние челове-ческого фактора на надежность защищенных телекоммуникационных систем; испытания систем на надежность				
Введение в дисциплину «Безопасность вычислительных сетей»	2	0	2	18
Основные понятия, термины и определения. Предмет и задачи дисциплины «Безопасность вычислительных сетей»				
Угрозы безопасности в компьютерных системах	8	4	4	22
Понятие угрозы. Угрозы безопасности информации в компьютерных системах. Понятия "идентификация", "аутентификация", "авторизация", "спе-цификация", "классификация", "категорирование" и "каталогизация". Класси-фикационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации — критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединения классов). Примеры и проблемы теоретического обоснования каталогов угроз по зарубежным, отечественным и международным стандартам				
Защищенные компьютерные и телекоммуникационные сети	8	4	4	22
Структура узлов ЗТКС. Основные принципы построения узлов связи как стационарных, так и полевых. Оперативно-технические службы узлов связи и их взаимодействие. Обеспечение и поставка техники на узлы связи. Хранение техники на узлах связи. Возможные каналы утечки информации при эксплуатации узлов ЗТКС. Основные каналы утечки информации. Методы технической защиты абонентских и соединительных линий на узлах связи. Методы защиты информации на элементах узлов связи ЗТКС				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
ИТОГО по 9-му семестру	36	16	18	108
10-й семестр				
Технологии обеспечения комплексной безопасности сетевых инфраструктур	10	4	6	18
Топология сети. Демилитаризованная зона. Хостинг во внешней организации. Сетевые элементы. Роутер и firewall. Системы обнаружения проникновения (IDS). Сетевые коммутаторы и концентраторы. Список действий для обеспечения безопасности сетевой инфраструктуры. Администрирование web-сервера. Создание логов. Основные возможности создания логов. Дополнительные требования для создания логов. Возможные параметры логов. Просмотр и хранение лог-файлов. Автоматизированные инструментальные средства анализа лог-файлов. Процедуры создания backup web-сервера. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация. SSL/TLS. Возможности SSL/TLS. Слабые места SSL/TLS. Пример SSL/TLS-сессии. Схемы шифрования SSL/TLS. Требования к реализации SSL/TLS. Список действий для технологий аутентификации и шифрования				
Модели безопасности на основе тематической и ролевой политик	8	4	4	18
Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств. Критерии безопасности информационных потоков в системах тематического разграничения доступа. Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными). Две фазы организации ролевого доступа — создание ролей как типовых субъектов доступа с наделением их правами				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
(полномочиями) доступа на основе дискреционной, мандатной, тематической или иной политики безопасности и назначение ролей пользователям				
Межсетевые экраны, пакетная фильтрация и обнаружение атак	10	4	4	18
Классификация firewall'ов. Установление TCP-соединения. Пакетные фильтры. Пограничные роутеры. Пример набора правил пакетного фильтра. Stateful Inspection firewall'ы. Host-based firewall'ы. Персональные firewall'ы и персональные устройства firewall'а. Основные характеристики пакетных фильтров в ОС FreeBSD. ПО пакетных фильтров. OpenBSD Packet Filter (PF) и ALTQ. Указание необходимости использования PF. Опции ядра. Опции rc.conf. Указание необходимости использования ALTQ. Создание правил фильтрации. IPFILTER (IPF) firewall. Понятие системы обнаружения атак. Почему следует использовать IDS. Типы IDS. Базовая архитектура IDS. Совместное расположение Host и Target. Разделение Host и Target. Способы управления IDS. Централизованное управление. Частично распределенное управление. Полностью распределенное управление. Скорость реакции. Информационные источники. Network-Based IDS. Host-Based IDS. Application-Based IDS				
Модели безопасности на основе дискреционной и мандатной политик	8	4	4	18
Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа. Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры. Модели разграничения доступа на основе матрицы доступа. Принудительный и добровольный принцип управления доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа. Общая характеристика политики				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
мандатного (полномочного) доступа. Парадигма градуированного доверия пользователям (субъектам доступа) и градуированной степени конфиденциальности данных (объектов доступа). Уровни безопасности субъектов и объектов доступа. Правила безопасного мандатного доступа — запрет чтения вверх (NRU) и запрет записи вниз (NWD). Рефрексивность, антисимметричность и транзитивность отношений доступа. Функция уровня безопасности субъектов и объектов доступа				
ИТОГО по 10-му семестру	36	16	18	72
ИТОГО по дисциплине	72	32	36	180