АННОТАЦИЯ ДИСЦИПЛИНЫ

«Безопасность открытых информационных систем»

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

Цели и задачи дисциплины

Целями освоения дисциплины «Безопасность открытых информационных систем- БОИС» является приобретение студентами фундаментальных представлений о функциях современной БОИС и о структуре ее функциональных компонентов, дается определение задач БОИС и ее границ, говорится об адекватном позиционировании и средствах интеграции БОИС в современной ИТ структуре. Современная проблема обеспечения безопасности информационных систем компаний, фирм, производств, Госучреждений является довольно сложным комплексом и объективными причинами появления этой проблемы и ее решения являются внутренние (сбои техники и программного обеспечения, ошибки и недоработки в проектировании, наладке систем, недостатки в масштабировании, обслуживания системы, администрирования мониторинга, аудита систем, преднамеренные и целенаправленные действия обслуживающего персонала, ведущие к нарушению сохранности информации), внешние (наличие объективных причин уязвимостей действующих систем и, как следствие, хакерские атаки и взлом систем) причины.. В курсе делается попытка создания единой системы обеспечения безопасности начиная от идеи создания такой системы, проектирования ее, наладке, эксплуатации и масштабирования. Отдельной темой будет раскрытие понятий, что такое система, информация ,безопасность, открытые и закрытые системы. ? Цели изучения дисциплины. • Уметь анализировать классы задач и процессов, создания защищенных информационных систем и навыков их поддержания ; • Описывать основные функциональные подсистемы и их взаимодействие в рамках комплексной БОИС; • Владеть методикой выбора средств автоматизации и методология процесса внедрения системы; • Знать разницу решения данной проблемы в отечественных организациях и зарубежных компаниях; • Понимать, персоналу разрешено все, что не запрещено, строгое соблюдение инструкций и этапов выполнение работ, уяснения понятия важности каждой должности в едином организме фирмы, справедливой системы материального поощрения; • Приобретение навыков в диагностировании работы алгоритмов, техники, протоколов, коррекция инструкций и положений; • Единое требование к безопасности- всеобщая система двойной парольной защиты, хранение любой информации в зашифрованном формате и система допуска к технике, программному обеспечению и атрибутам информации..

Изучаемые объекты дисциплины

Открытые информационные системы.

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		10	11
1. Проведение учебных занятий (включая проведе-ние текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	126	72	54
- лекции (Л)	60	36	24
- лабораторные работы (ЛР)	32	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	30	18	12
- контроль самостоятельной работы (КСР)	4	2	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	126	72	54
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет	9		9
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	288	180	108

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
10-й семестр				
Математические, технические, прооамные средства обеспечения (БИС)	18	8	8	36
2.1. Администрирование, масштабирование, настройка (БИС) 2.2. Настройка экранов. Брандмауэров, антивирусная защита.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Методологические основы обеспечения безопасности информационных систем (БИС)	18	8	10	36
1.1 Философское трактование понятий открытых и закрытых систем и подсистем 1.2. Архитектура и основы (БИС) 1.3. Концепсия. (БИС) 1.4.Теоретические основы утентификации 1.5.Основные положения управление доступа к элеменам информации. 1.6.Понятие положений конфиденциальности, сохранности, ответственности и авторства информации 1.7.Обеспечение основ мониторинга и аудита (БИС) 1.8. Криптографические основы (БИС)				
ИТОГО по 10-му семестру	36	16	18	72
11-й семестр				
Основные положения способы создания защищенных сетей на базе сетей интернета.	24	16	12	54
1.Сети Win VPN, OpenVpn., Cisko Pacet Tracer. 1.2. Моделирование . (БИС) На основе Virtual Box. 1.3. Моделирование . (БИС) На основе OpenVpn/ .1.4. Моделирование . (БИС) На основе. Cisko Pacet Tracer 1.5. Построение сетей в терминальных классах. 1.6. Построение сетей на оборудовании домашних компьютеров студентов. 1.7.Организация систем удаленного доступа				
ИТОГО по 11-му семестру	24	16	12	54
ИТОГО по дисциплине	60	32	30	126