АННОТАЦИЯ ДИСЦИПЛИНЫ

«Методы и средства обнаружения компьютерных атак»

Дисциплина «Методы и средства обнаружения компьютерных атак» является частью программы магистратуры «Компьютерные системы и сети» по направлению «09.04.01 Информатика и вычислительная техника».

Цели и задачи дисциплины

Знакомство с системами обнаружения атак и защиты информации. Изучение событий безопасности. Освоение способов обнаружения аномалий. Освоение современные методы анализа данных. Изучение алгоритмов обучения классификаторов. Освоение уровни сети согласно OSI. Создание систем противодействия угрозам безопасности. Знакомство с признаками нарушения безопасности информации..

Изучаемые объекты дисциплины

Система обнаружения атак Защита информации События безопасности Безопасность информации Способы обнаружения аномалий Современные методы анализа данных Алгоритмы обучения классификаторов Уровни сети согласно OSI Создание и противодействие угрозам безопасности Признаки нарушения безопасности информации.

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		4
1. Проведение учебных занятий (включая проведе-ние текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	72	72
- лекции (Л)	18	18
- лабораторные работы (ЛР)	24	24
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	26	26
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	72	72
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
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
4-й семестр				
Методы ВИ для обнаружения и классификации аномальных сетевых соединений	6	8	8	24
Модель искусственной "иммунной системы" на базе эволюционного подхода Алгоритм генетико-конкурентного обучения сети Кохонена Модели и алгоритмы обучения бинарных классификаторов Методика иерархической гибридизации бинарных классификаторов для обнаружения аномальных сетевых соединений				
Системный анализ проблемы обнаружения и классификации сетевых атак	6	8	8	24
Классификация методов обнаружения сетевых атак Место и роль методов ВИ в областях ИИ и обнаружения аномальных сетевых соединений Классификация СОА и архитектура распределенной СОА Требования, предъявляемые к СОА Постановка задачи исследования				
Программная реализация СОА и экспериментальная оценка ее эффективности	6	8	10	24
Компоненты обнаружения сетевых атак на основе сигнатурного анализа Архитектура и программная реализация распределенной СО Экспериментольное исследование реализации распределенной СО				
ИТОГО по 4-му семестру	18	24	26	72
ИТОГО по дисциплине	18	24	26	72