АННОТАЦИЯ ДИСЦИПЛИНЫ

«Интеллектуальные средства обнаружения и блокировки»

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

Цели и задачи дисциплины

Знакомство студентов с современными средствами обнаружения и блокировки компьютерных атак. Разработка средств противодействия..

Изучаемые объекты дисциплины

Архитектура системы обнаружения атак. Базы знаний, база методов и сигнатур. Блоки построения дерева принятия решений. Методы понижения вероятности ошибки. Классификация и виды атак. Способы выявления атак (сигнатурный, на основе аномалий, глубокий анализ траффика). Ситуации нарушения доступности, конфиденциальности и целостности. Обучение нейросети и наборы данных Система обнаружения атак / обнаружения вторжений..

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				
Системы обнаружения вторжений на основе нейросетей	3	4	4	12
Системы обнаружения вторжений на основе нейросетей Обзор и классификация СОВ. Исследование работы типовой СОВ				
Использование схемы совпадений в системах обнаружения вторжений на основе нейронных сетей	3	4	4	12
Обучение и сравнение результатов различных классификаторов. Получение общего предсказания типа атаки. Оценка эффективности в сравнении с другими методами.				
Возможные варианты построения интеллектуальной системы обнаружения несанкционированной работы программного обеспечения	3	4	6	12
Сигнатурный метод анализа Контроль работы программ по профилям Использование прогнозируемых шаблонов Метод обнаружения опасных комбинаций безопасных событий Анализ переходов системы из состояния в состояние Контроль превышения пороговой величины частоты событий Статистический анализ последовательности системных вызовов Продукционные и экспертные системы				
Подготовка данных для использования в обучении и тестировании нейросетей при обнаружении сетевых атак	3	4	4	12
Способы захвата траффика. Способы противодействия захвату. Исследование ПО для захвата и классифицирования траффика.				
Особенности использования искусственных нейронных сетей в сфере информационной безопасности	3	4	4	12
Стадии атаки. Выявление признаков атаки. Подготовка обучающих данных. Эксперименты по обнаружению типовых атак.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Анализ зашифрованного сетевого трафика на основе вычисления энтропии и применения нейросетевых классификаторов	3	4	4	12
Методы получения признаков траффика Вычисление энтропии сигнала Нейросетевые методы классификации траффика Оценка пригодности метода				
ИТОГО по 4-му семестру	18	24	26	72
ИТОГО по дисциплине	18	24	26	72