

Аннотация к рабочей программе дисциплины «Теория псевдослучайных генераторов»

Курс учебной дисциплины «Теория псевдослучайных генераторов» разработан для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.13.02.

Общая трудоемкость курса 4 зачетные единицы, 144 академических часа. Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (18 час.), практические занятия (18 час.), самостоятельная работа (36 час.), подготовка к экзамену (36 час.). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Теория псевдослучайных генераторов» логически и содержательно связана с такими курсами, как «Математическая логика и теория алгоритмов», «Алгебра», «Теория вероятностей и математическая статистика», «Языки программирования».

Дисциплина «Теория псевдослучайных генераторов» обеспечивает приобретение знаний и умений в области алгоритма генератора псевдослучайных чисел, порождающего последовательность чисел, элементы которой подчиняются заданному распределению. Изучение этой дисциплины способствует освоению принципов применения генератора псевдослучайных чисел в информатике – от метода Монте-Карло и имитационного моделирования до криптографии.

Цель - подготовка обучающихся к научно-исследовательской деятельности в областях, использующих математические методы и компьютерные технологии, а также работе в сфере защиты информации.

Задачи:

- изучить основные определения и понятия теории псевдослучайных генераторов;

- изучить основные способы построения псевдослучайных генераторов;

- разрабатывать и анализировать математические модели процессов с использованием генератора псевдослучайных чисел.

Для успешного изучения дисциплины «Теория псевдослучайных генераторов» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

- способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);

- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессионально-специализированные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	основные прикладные аспекты псевдослучайных генераторов
	Умеет	разрабатывать формальные модели политик безопасности
	Владеет	навыками разработки формальных моделей политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации

(ПСК-2.1) способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает	основные определения и понятия теории псевдослучайных генераторов
	Умеет	разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации
	Владеет	основными терминами предметной области
(ПСК-2.2) способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знает	основные способы построения псевдослучайных генераторов
	Умеет	оценивать эффективность средств и методов защиты информации в компьютерных системах
	Владеет	способностью анализировать применяемые математические методы и алгоритмы
(ПСК-2.4) способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает	принципы построения и свойства псевдослучайных генераторов
	Умеет	разрабатывать математические модели процессов
	Владеет	основными знаниями в области теории псевдослучайных генераторов

Для формирования вышеуказанных компетенций в рамках дисциплины «Теория псевдослучайных генераторов» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).