АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Теория псевдослучайных генераторов»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- ознакомление студентов с основными понятиями теории генераторов псевдослучайных чисел;
- развитие навыка построения генераторов псевдослучайных чисел.

Задачи освоения дисциплины:

- овладение основными идеями и методами построения генераторов псевдослучайных чисел;
- формирование навыков грамотного применения основ теории генераторов псевдослучайных чисел в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к факультативной части цикла ФТД (ФТД.2) образовательной программы и читается в 9-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра», «Дискретная математика», «Информатика», «Криптографические методы защиты информации».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Дисциплина «Теория псевдослучайных генераторов» является предшествующей для прохождения преддипломной практики и итоговой государственной аттестации.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Процесс изучения дисциплины «Вычислительные методы в алгебре и теории чисел» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-1 – способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в	Знать: методы построения криптографических генераторов псевдослучайных чисел; Уметь: решать задачи на построение криптографического

том числе на иностранном языке	генератора псевдослучайных чисел; разрабатывать быстрые вычислительные алгоритмы построения генераторов псевдослучайных чисел для криптографических приложений; Владеть: терминологией теории генераторов псевдослучайных чисел
ПК-6 – способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Знать: методы построения криптографических генераторов псевдослучайных чисел; Уметь: решать задачи на построение криптографического генератора псевдослучайных чисел; разрабатывать быстрые вычислительные алгоритмы построения генераторов псевдослучайных чисел для криптографических приложений; Владеть: терминологией теории генераторов псевдослучайных чисел
ПК-7 – способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Знать: методы построения криптографических генераторов псевдослучайных чисел; Уметь: решать задачи на построение криптографического генератора псевдослучайных чисел; разрабатывать быстрые вычислительные алгоритмы построения генераторов псевдослучайных чисел для криптографических приложений; Владеть: терминологией теории генераторов псевдослучайных чисел
ПК-8 – способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Знать: методы построения криптографических генераторов псевдослучайных чисел; Уметь: решать задачи на построение криптографического генератора псевдослучайных чисел; разрабатывать быстрые вычислительные алгоритмы построения генераторов псевдослучайных чисел для криптографических приложений; Владеть: терминологией теории генераторов псевдослучайных чисел
ПК-18 – способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	Знать: методы построения криптографических генераторов псевдослучайных чисел; Уметь: решать задачи на построение криптографического генератора псевдослучайных чисел; разрабатывать быстрые вычислительные алгоритмы построения генераторов псевдослучайных чисел для криптографических приложений; Владеть: терминологией теории генераторов псевдослучайных

	чисел

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение зачета.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к семинарам, их оформление;
- подготовка к лабораторным работам, их оформление.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: лабораторные работы, проверка решения задач.

Промежуточная аттестация проводится в форме: зачет.