Аннотация к учебной программе дисциплины

«Методы алгебраической геометрии в криптографии»

Рабочая программа учебной дисциплины «Методы алгебраической геометрии в криптографии» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана с кодом Б1.Б.13.03.

Общая трудоемкость освоения дисциплины составляет 180 часов (5 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (18 часов), лабораторные работы (36 часов), самостоятельная работа (90 час., в том числе 36 часов на подготовку к экзамену). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Геометрия», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теоретико-числовые методы в криптографии».

Курс «Методы алгебраической геометрии в криптографии» составляет одну из фундаментальных частей современной теоретической криптографии, без знания которых невозможна дальнейшая профессиональная подготовка в области современной защиты информации. При освоении данного курса у студентов формируются навыки грамотного применения теоретических основ криптографии в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

Цели:

- сформировать представление о комплексе идей и методов классической геометрии плоскости и пространства
- выработать у студентов умения применять основные приёмы геометрических методов при исследовании математических моделей, возникающих в естествознании и прикладных науках, развить математическую культуру студента и подготовить его к усвоению других основных

математических курсов.

Задачи:

- последовательное изложение теоретического материала на лекциях, при котором все основные результаты снабжаются строгими доказательствами;
- отработка приемов решения задач на практических занятиях.

Для успешного изучения дисциплины «Методы алгебраической геометрии в криптографии» 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 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, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-10) способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знает	базовые структуры данных; современные технологии программирования
	Умеет	планировать разработку сложного программного обеспечения; проводить оценку сложности алгоритмов; разрабатывать эффективные алгоритмы и программы
	Владеет	навыками документирования программного обеспечения; навыками разработки алгоритмов решения типовых профессиональных задач

ПСК-2.2 способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знает	основные понятия алгебраической геометрии: аффинные и проективные пространства, алгебраические многообразия, дивизоры, и т.д
	Умеет	оценивать качество криптографической защиты
	Владеет	навыками криптоанализа асимметричных систем шифрования
ПСК-2.3 способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает	принципы применения эллиптических и гиперэллиптических кривых в криптографии
	Умеет	разрабатывать быстрые вычислительные алгоритмы для криптографических приложений
	Владеет	навыками программирования алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических и гиперэллиптических кривых
ПСК-2.5 способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации	Знает	принципы и методы построения быстрых алгоритмов для реализации систем защиты информации
	Умеет	проводить предварительное оценивание временной сложности разрабатываемых алгоритмов
	Владеет	методами алгебраической геометрии в криптографии

Для формирования вышеуказанных компетенций в рамках дисциплины «Методы алгебраической геометрии в криптографии» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспект (ПР-7), собеседование (ОУ-1),

коллоквиум (ОУ-2), лабораторные работы (ПР-6).