Аннотация к рабочей программы дисциплины

«Б1.В.06. Криптографические методы защиты информации»

(код и наименование дисциплины)

Объем трудоемкости: 4 зачетных единицы

Цель дисциплины: проблемы информатизации и защиты информации средствами криптографии. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук.

Место дисциплины в структуре образовательной программы

Дисциплина «криптографические методы защиты информации» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана Б1.В.06.

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-5 способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) средств защиты информации	
ПК-5.1 Организует информационную среду в соответствии с правовыми нормами и регламентами профессиональной деятельности учреждения или организации ПК-5.2 Владеет основами информационных технологий, умеет профессионально определить уровень необходимого программно-аппаратного обеспечения защищаемой информационной системы ПК-5.3 Имеет навыки установки, тестирования и обновления программно-аппаратного оснащения администрируемой информационной системы (сети)	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.
ПК-4 Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	
ПК-4.1 Умеет применять и реализовывать математически сложные алгоритмы в современных программных комплексах ПК-4.2 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике и естественных науках ПК-4.3 Демонстрирует умение отбора среди существующих методов наиболее подходящие для решения конкретной прикладной задачи	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа. Элементы теории сложности алгоритмов. Уметь: Определять структуры данных в компьютерной алгебре. Использовать технику символьных вычислений. Применять основные математические методы, используемые в анализе типовых криптографических алгоритмов. Владеть навыками: классификации систем компьютерной алгебры; ориентироваться в типовых архитектурах вычислительных процессов;

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
	использования библиотеки алгоритмов и пакетов расширения;

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	20	2		2	16
2.	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	24	4		4	16
3.	Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами	22	2		4	16
4.	Системы шифрования с открытыми ключами	28	4		4	20
5.	*Итого по дисциплине:*		12		14	68
	Контроль самостоятельной работы (КСР)	-				
	Промежуточная аттестация (ИКР)	0,3				
	Подготовка к текущему контролю	35,7				
	Общая трудоемкость по дисциплине	144				

Курсовые работы: предусмотрена

Форма проведения аттестации по дисциплине: зачет

Автор А.В. Рожков, профессор, д.ф.-м.н., профессор