АННОТАЦИЯ
дисциплины «Б1.В.03 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Объем трудоемкости: 3 зачетные единицы (108 часов, из них – 74,2 часа контактной работы (30 часов лекций, 30 практических занятий, 14 курсовая работа, 0,2 часа ИКР); 33,8 часов самостоятельной работы).

Цель дисциплины:

Цель освоения дисциплины – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

Задачи дисциплины:

Задачи освоения дисциплины «Криптографические методы защиты информации»: 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, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета и получение сведений:

о нормативных требованиях по административно-правовому регулированию в области криптографической защиты информации;

об основных задачах и понятиях криптографии;

об этапах развития криптографии;

о видах информации, подлежащей шифрованию;

о классификации шифров;

о методах криптографического синтеза и анализа;

о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;

о методах криптозащиты компьютерных систем и сетей.

Место дисциплины в структуре ООП ВО

Дисциплина «Криптографические методы защиты информации» относится к вариативной части блока Б1 Дисциплины (модули) и является обязательной дисциплиной.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-6	Способностью к собственному ведению прикладного аспекта в строгих математических формулировках.	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа.	Применять основные математические методы, используемые в анализе типовых алгоритмов.	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

Основные разделы дисциплины: Разделы дисциплины, изучаемые во 2 семестре

№ раз-дела	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Самостоя-тельная работа
			Л	Пр	
1	**2**	**3**	**4**	**5**	**6**
1	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	32	8	8	6
2	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	26	8	8	10
3	Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами	18	6	6	6
4	Системы шифрования с открытыми ключами	25,8	8	8	11,8
	Итого:		30	30	33,8

Курсовые работы: предусмотрена.
Форма проведения аттестации по дисциплине: зачет
Основная литература:

1. Рябко Б.Я, Фионов А.Н. Основы современной криптографии и стеганографии, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2013. - URL: https://e.lanbook.com/book/63244
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: https://e.lanbook.com/book/70724

Автор РПД Рожков А.В.