Аннотация к рабочей программе дисциплины
Б1.В.ДВ.4.2 Математические основы кодирования информации
направление подготовки 09.03.03 Прикладная информатика
(профиль «Прикладная информатика в машиностроении»)

Дисциплина Б1.В.ДВ.4.2 Математические основы кодирования информации изучается во 2 семестре. Предусмотрены лекционные и семинарские занятия. Отчетность по результатам освоения дисциплины – зачет.

Цель освоения дисциплины – формирование знаний и умений в теории кодирования, в частности в области криптографии.

Место дисциплины в структуре образовательной программы.

Дисциплина «Математические основы кодирования информации» относится к дисциплинам по выбору вариативной части Блока 1 Дисциплины (модули) (Б1.В.ДВ.4.2).

Содержание дисциплины «Математические основы кодирования информации» опирается на дисциплину «Математический анализ» (Б1.Б.13).

Содержание дисциплины «Математические основы кодирования информации» выступает опорой для освоения содержания дисциплины «Теоретические основы информатики» (Б1.В.ДВ.2.1).

Планируемые результаты освоения образовательной программы			
Код компетенции	**Наименование компетенции**	**Структурные элементы компетенции**	**Результаты обучения по дисциплине**
ОПК-2	способность анализировать социально-экономические задачи и процессы с применением методов системного анализа и математического моделирования	**З1(ОПК-2):** основные математические понятия;	*знать:* – наиболее широко используемые классы шифров (блочные, вероятностные, цифровая подпись и др.);
		У1(ОПК-2): применять методы математики для решения практических задач;	*уметь:* – проектировать шифры; – применять математический аппарат, используемый в криптографии;
		В1(ОПК-2): методами и приемами математики для решения задач профессиональной деятельности;	*владеть:* – основными приемами и методами проектирования шифров; – основными приемами и методами проектирования цифровой подписи;
ПК-2	способность разрабатывать, внедрять и адаптировать прикладное программное обеспечение	**З1(ПК-2):** основные методы и подходы к разработке прикладного ПО;	*знать:* – методы построения цифровой подписи; методы управления ключами;
		У2(ПК-2): разрабатывать и реализовывать прикладное ПО.	*уметь:* – использовать знания по криптографии в профессиональной деятельности.

Разделы дисциплины включают:

1. Проблематика криптографии и симметричные шифры.
2. Двухключевые криптосистемы
3. Системы ЭЦП с составным модулем
4. Открытое распределение ключей и открытое шифрование.
5. Хэш-функции
6. Управление ключами и протоколы

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Составитель – к.п.н., доцент кафедры физико-математического и информационно-технологического образования И.Н. Слинкина.