

**Аннотация к рабочей программе дисциплины
 Б1.В.ДВ.4.2 Математические основы кодирования информации
 направление подготовки 09.03.01 Информатика и вычислительная техника
 (Профиль "Программное обеспечение вычислительной техники и автоматизированных систем")**

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 дисциплин «Теоретические основы информатики» (Б1.В.ДВ.2.1).

Планируемые результаты освоения образовательной программы			
Код компетенции	Наименование компетенции	Структурные элементы компетенции	Результаты обучения по дисциплине
ПК-2	способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования	З2 (ПК-2): теоретические основы организации и проектирования аппаратно-программных комплексов и баз данных.	<i>знать:</i> – наиболее широко используемые классы шифров (блочные, вероятностные, цифровая подпись и др.); – методы построения цифровой подписи; методы управления ключами;
		У1 (ПК-2): разрабатывать компоненты аппаратно-программных комплексов.	<i>уметь:</i> – уметь проектировать шифры; – уметь применять математический аппарат, используемый в криптографии; использовать знания по криптографии в профессиональной деятельности.
СК-1	способность использовать естественно-научные и математические знания в профессиональной деятельности	З1(СК-1): основные математические понятия;	<i>знать:</i> - математический аппарат дисциплины для расчета и проектирования аппаратно-программных комплексов и баз данных.

Планируемые результаты освоения образовательной программы			
Код компетенции	Наименование компетенции	Структурные элементы компетенции	Результаты обучения по дисциплине
		У1(СК-1): применять математические методы для решения задач в профессиональной деятельности;	<i>уметь:</i> - применять математический аппарат дисциплины в процессе разработки аппаратно-программных комплексов и баз данных.

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 И.Н. Слинкина.