Аннотация дисциплины

Наименование дисциплины	**Математические основы криптологии**
Содержание	Введение в криптологию. Основы теории делимости. Расширенный алгоритм Евклида. Решение линейных диофантовых уравнений. Модульная арифметика. Нахождение мультипликативной инверсии. Решение уравнений сравнения. Операции над матрицами вычетов. Малая теорема Ферма. Теорема Эйлера. Алгоритмы генерации простых чисел. Детерменированные и вероятностные алгоритмы проверки чисел на простоту. Разложение чисел на простые множители. Модульное возведение в степень. Китайская теорема об остатках. Алгебраические основы криптологии: группы, кольца, поля, полиномы над структурой, эллиптические кривые.
Реализуемые компетенции	способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2) способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)
Результаты освоения дисциплины (модуля)	**ОПК-2** **Знать:** сведения из математических дисциплин, позволяющие решать профессиональные задачи, **Уметь:** применять соответствующий математический аппарат для решения профессиональных задач, **Владеть:** методами из математических дисциплин для решения профессиональных задач. **ПК-1** **Знать:** требования по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; **Уметь: у**станавливать, настраивать и обслуживать программные, программно-аппаратные (в том числе криптографические) и технические средства защиты информации; **Владеть:** способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Трудоемкость, з.е.	4 з.е.
Форма отчетности	Экзамен – 5 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Гашков, С. Б. Криптографические методы защиты информации [Текст]:.- М.: ИЦ "Академия", 2012. 2. Введение в теоретико-числовые методы криптографии [Текст]: учебное пособие / М.М. Глухов [и др.]. - СПб.: "Лань", 2013.
Дополнительная литература	1. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие/ В.П. Мельников, С.А. Клейменов, А.М. Петраков - М.: ИЦ "Академия", 2012. 2. Ярочкин В.И. Информационная безопасность: учебник для вузов/ В.И. Ярочкин - М.: Академический Проект, 2013.