Аннотация дисциплины

Наименование дисциплины	**Безопасность баз данных**
Содержание	Основные понятия криптографии. Классические шифры замены. Классические шифры перестановки. Принципы построения современных шифров с симметричным ключом. Современные стандарты симметричного шифрования DES, AES, ГОСТ 28147-89, ГОСТ Р 34.12-2015. Современные алгоритмы шифрования с открытым ключами. Криптосистемы RSA, Эль-Гамаля, Рабина. Алгоритмы генерации простых чисел. Проверка чисел на простоту. Сложность криптографических алгоритмов. Аутентификация данных. Электронная цифровая подпись. Алгоритмы ЭЦП: RSA, Эль-Гамаля, Шнорра, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012. Атаки и угрозы схемами ЭЦП. Понятие о структуре и способах построения криптографических протоколов. Классификация криптографических протоколов.
Реализуемые компетенции	способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2); способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4); способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем (ПСК-2).
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-4** **Знать:** реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; **Уметь:** участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; **Владеть:** способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты. **ПСК-2** **Знать:** современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем; **Уметь:** применять современные информационные технологии и

	методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем; **Владеть:** способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем.
Трудоемкость, з.е.	5 з.е.
Форма отчетности	Экзамен – 6 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Петров А.А. Компьютерная безопасность. Криптографические методы защиты.- Саратов: Профобразование, 2017.- 446 с.
Дополнительная литература	1. Лапонина О.Р. Криптографические основы безопасности.- Москва: ИНТУИТ, 2016.- 244 с. 2. Калмыков И.А. Криптографические методы защиты информации.- Ставрополь: СКФУ, 2015.- 109 с.