Аннотация дисциплины Б1.Б.22
«Криптографические методы защиты информации»
Общая трудоемкость изучения дисциплины составляет 5 ЗЕТ (180 часа)

Целью дисциплины: дать будущим инженерам, специализирующимся в области защиты информации, основы знаний о принципах защиты информации с помощью криптографических методов и особенностях реализации этих методов на практике.

Задачи дисциплины:

- дать студентам основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов;
- дать студентам основы принципов анализа и синтеза шифров;
- ознакомить студентов с математическими методами, используемыми в криптографии;

Основные дидактические единицы (разделы): Введение в криптографию. Имитостойкость и помехоустойчивость шифров. Принципы построения и реализации криптографических алгоритмов. Шифрование с открытым ключом. Криптографические протоколы. Криптосистемы на базе ЭВМ.

Компетенции, приобретаемые в процессе изучения дисциплины

способностью к самоорганизации и самообразованию (ОК-8);

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

В результате изучения дисциплины студент должен:

Знать:

основные криптографические протоколы системы шифрования с открытыми ключами;

о принципиальных подходах к созданию современных технических средств криптографической защиты информации;

основные стандарты, протоколы и интерфейсы, используемые в автоматизированных системах;

криптографические средства и системы защиты информации и их программно-аппаратную реализацию;

Уметь:

использовать свойства криптографических средств при анализе комплексных систем защиты информации;

оценивать уязвимость протоколов и интерфейсов компьютерных систем;

оценивать криптографическую стойкость шифров;

применять криптографические средства и системы информационной безопасности;

Владеть:

государственными (национальными) стандартами, регулирующими криптографические методы защиты информации в ведущих странах;

основными принципами построения аппаратных и программных реализации криптографических алгоритмов;

криптографическими средствами и базовыми технологиями информационной безопасности;

методами оценки криптографической стойкости алгоритмов шифрования;

типовыми криптографическими протоколами и их криптографическими качествами;

навыками рационального выбора средств и методов защиты информации объектов информатизации.

Виды учебной работы:

Семестр	Часов							ЗЕТ
	Всего	Контактная работа (по уч. зан.)				Самост. работа	Контроль	
		Всего	Лек	Лаб	Пр			
	180	72	36		36	72	36	5

Изучение дисциплины заканчивается в восьмом семестре экзаменом и курсовым проектом