Аннотация

учебной дисциплины Б1.В.06 Криптографические методы защиты информации

направления подготовки бакалавров 10.03.01. Информационная безопасность

Дисциплина учебного плана подготовки бакалавра по направлению 10.03.01. Информационная безопасность, профиль «Организация и технология защиты информации»

Цель изучения курса:

Основной целью дисциплины «Криптографические методы и средства защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачами курса являются:

дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; изучение принципов разработки шифров, математических методов, используемых в криптографии.

Основные блоки и темы дисциплины:

Введение в криптографию. Основные классы шифров. Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом. Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Хеш-функции и их криптографические приложения.

Учебная дисциплина «Криптографические методы защиты информации» входит в перечень дисциплин базовой части ОП.

Дисциплина «Криптографические методы и средства защиты информации» обеспечивает изучение дисциплины: «Защита информации». Знания и практические навыки, полученные из дисциплины «Криптографические методы и средства защиты информации», используются обучаемыми при разработке дипломных работ.

В результате изучения дисциплины бакалавр должен обладать следующими компетенциями:

Знать: о видах и формах информации, ее уязвимостях, механизмах реализации различных угроз; структуре и содержании информационных процессов и методах их анализа (ПК-1).

Уметь: выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-2).

Владеть: навыками проведения анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов. (ПК-7).

Дисциплина изучается посредством лекций, все разделы программы закрепляются практическими занятиями, контрольной работы, самостоятельной работы над учебной и научно-технической литературой.

Общая трудоемкость дисциплины составляет **252 часа, 7 зачетных единицы.**

Вид промежуточной аттестации: зачет, экзамен.

Разработчик:

к.э.н., доцент _____ А.А.Киздермишов

Зав. выпускающей кафедрой

по направлению _____ С.Г. Чефранов