Аннотация

рабочей программы учебной дисциплины Б1.Б.19 «Криптографические методы защиты информации»

специальности 10.05.04 Информационно-аналитические системы безопасности

специализация N2 «Информационная безопасность финансовых и экономических структур»

Цель изучения курса:

Основной целью дисциплины «Криптографические методы 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 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-15).

Уметь: выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-15).

Владеть: навыками проведения анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов. (ПК-15).

Дисциплина Криптографические методы защиты информации» изучается посредством лекций, все разделы программы закрепляются лабораторными занятиями, контрольной работы, самостоятельной работы над учебной и научно-технической литературой.

Общая трудоемкость дисциплины составляет **108 часов, 3 зачетных единицы.**

Вид промежуточной аттестации: зачет.

Разработчик А.А. Киздермишов

Зав. выпускающей кафедрой В.Ю. Чундышко