

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ  
УНИВЕРСИТЕТ

**Институт систем управления**

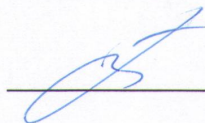
Кафедра прикладной информатики и информационной безопасности

**АННОТАЦИЯ**

по дисциплине **«Криптографические методы защиты информации»**

**направление подготовки 10.03.01 Информационная безопасность  
профиль «Организация и технология защиты информации»  
очной формы обучения**

Соответствует РПД



Зав. кафедрой

  
/Абросимов А.Г./

Самара 2015 г.

## 1. Цели и задачи дисциплины

Дисциплина «Криптографические методы защиты информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления. Целью изучения дисциплины «Криптографические методы защиты информации» является освоение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины – дать основы:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов синтеза и анализа шифров;
- математических методов, используемых в криптоанализе.

## 2. Место дисциплины в структуре ООП

Изучение дисциплины «Криптографические методы защиты информации» базируется на следующих дисциплинах: «Математика (математический анализ, алгебра, геометрия)», «Теория вероятностей и математическая статистика», «Дискретная математика», «Теория информации», «Информатика», «Основы информационной безопасности».

Дисциплина «Криптографические методы защиты информации» обеспечивает изучение следующих дисциплин: «Техническая защита информации», «Информационная безопасность корпоративных автоматизированных информационных систем», «Комплексная система защиты информации на предприятии». Знания и практические навыки, полученные из дисциплины «Криптографические методы защиты информации», используются обучаемыми при разработке курсовых и дипломных работ.

## 3. Требования к уровню освоения содержания дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

общекультурных

ОК-11	способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства
-------	---

профессиональных (ПК):

ПК-23	способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности
ПК-27	способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

В результате изучения дисциплины студенты должны:

**иметь представление:**

- об истории криптографии;

- о классификации шифров;
- о подходах к оценке стойкости шифров;
- о методах синтеза и анализа шифров;
- о криптографических методах аутентификации и удостоверения авторства;
- о государственных стандартах в области криптографии;

**знать:**

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- типовые поточные и блочные шифры и шифры с открытыми ключами;
- простейшие криптографические протоколы;
- частотные характеристики открытых текстов и их применение к анализу простейших шифров замены и перестановки;

**уметь:**

- применять математические методы описания и исследования шифров;
- оценивать криптографическую стойкость шифров;

**владеть:**

- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- навыками математического моделирования в криптографии;
- навыками работы с научно-технической литературой в области криптографии.

**4. Объем дисциплины и виды учебной работы**

<b>Вид учебной работы</b>	<b>Всего часов/зачетных единиц</b>	<b>Семестр 3</b>
Аудиторные занятия	72/2	72/2
В том числе:		
Лекции	36/1	36/1
Практические занятия (ПЗ)	36/1	36/1
Семинары (С)		
Лабораторные работы (ЛР)		
Самостоятельная работа (всего)	45/1,25	45/1,25
В том числе:		
Курсовой проект	36/1	36/1
Расчетно-графические работы		
Реферат		
Другие виды самостоятельной работы	9/0,25	9/0,25
Вид промежуточной аттестации (экзамен)	27/0,75	27/0,75
Общая трудоемкость	144 /4	144 /4