

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

(название дисциплины)

10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

5

(семестр)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- «Криптографические методы защиты информации» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность», ознакомление студентов с основами теории двоичного кодирования, алгоритмами сжатия, помехоустойчивого кодирования. Дисциплина «Криптографические методы в защите информации» рассматривается как теоретическая и прикладная дисциплина, дающая представления об основных математических и алгоритмических подходах, применяемых для хранения, передачи, исправления информации, представленной в двоичных кодах. Дисциплина посвящена изучению основ криптографии и криптографического анализа, применяемых к защите информации в информационных системах. Обучаемые знакомятся с понятием шифров, симметричной и асимметричной криптографии, электронной подписью, хешированием и другими математическими объектами криптографии. Изучаются соответствующие криптографические стандарты, применяемые сегодня в защите информации в России и за рубежом. Подробно рассматриваются: стандарты RSA, DES, GOST1989, и другие. Также уделено внимание перспективным направлениям в криптографии: криптографические протоколы с разглашением и без разглашения, теория алгоритмической сложности и односторонних функций, схемы разделения секрета и некоторые их приложения в задачах идентификации и аутентификации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

- Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.8). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.
- Дисциплина изучается на 3 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Математика», «Информатика» по направлению подготовки 10.03.01 «Информационная безопасность», квалификации - бакалавр. Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Основы информационной безопасности», «Техническая защита информации», «Программно-аппаратные средства защиты информации», «Математические методы в информационной безопасности», «Защита информации в корпоративных ИС» и т.д..

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе освоения дисциплины студент формирует и демонстрирует следующие общекультурные и общепрофессиональные способности:

- ОПК-2 – способностью применять соответствующий математический аппарат для решения профессиональных задач;
- ПК-1 – способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- ПК-12 – способностью принимать участие в проведении экспериментальных исследований системы защиты информации.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Введение. Основные задачи криптологии. Криптография и криптографический анализ

Открытый и закрытый тексты, ключ, основные свойства функции шифрования и дешифрования. Примеры шифров. Шифр Цезаря, Полибия

Симметричные шифры. Группы подстановок и перестановок. Чистые шифры. Шифры Виженера и Вернама. Одноразовый блокнот. Теорема Шеннона об абсолютно стойком шифре. Принцип Керкхоффа. Проблемы симметричной криптографии.

Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий.

Блочные Шифры. Стандарты DES, GOST1989. Поточные шифры. Стандарт А5.

Асимметричная криптография. Классы алгоритмической сложности. Сложность математических задач.

- Односторонние функции
Задачи факторизации и дискретного логарифма. Функция Эйлера. RSA. Электронная подпись.
- Криптографические протоколы. Протокол анонимных вычислений. Схемы разделения секрета. Криптография на эллиптических кривых

Составитель: доцент кафедры ИЗИ к.ф.-м.н. Александров А. В

должность, ФИО, подпись

Заведующий кафедрой ИЗИ

М.Ю. Монахов

ФИО, подпись

Директор института ИТР

А.А. Галкин

ФИО, подпись

Дата, Печать института (факультета)

