АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

КРИПТОЛОГИЯ

(название дисциплины)

10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

5,6,7

(семестр)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- Целями освоения дисциплины «Криптология» 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 «Криптология» 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.
- Задачами изучения дисциплины «Криптология» являются: -ознакомление с основами математической теории криптологии; - приобретение навыков в практическом использовании, постановке и решении задач шифрования информации; - понимание сути информационных процессов в криптографических системах; - применение компьютеров для решения задач шифрования и дешифрования; - разработка и использование математических и вычислительных моделей процессов шифрования информации, их оптимизация и выработка направлений совершенствования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

- Данная дисциплина относится к базовой части Блока Б1 (код Б1.Б.05). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и практических занятий.
- Дисциплина изучается на 3 и 4 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Математика», «Информатика» по направленности 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».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими общекультурными и профессиональными компетенциями:

- 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-2 - способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

- Введение. Основные задачи криптологии. Криптография и криптографический анализ

- Открытый и закрытый тексты, ключ, основные свойства функции шифрования и дешифрования. Примеры щифров. Шифр Цезаря, Полибия
- Симметричные шифры. Группы подстановок и перестановок.
- Чистые шифры. Шифры Виженера и Вернама.
- Одноразовый блокнот. Теорема Шеннона об абсолютно стойком шифре.
- Принцип Керкхоффса. Проблемы симметричной криптографии.
- Хеш - функции. Хеш - функции,
- Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий. Парадокс о днях рождения
- Блочные Шифры. Стандарты DES
- Стандарт GOST1989. Поточные шифры. Стандарт A5.
- 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
- Криптографический анализ
- Пассивный криптографический анализ
- Частотный анализ
- Дифференциальный и линейный криптографический анализ
- Активный криптоанализ
- Пороговые схемы разделения
- Протокол анонимных вычислений
- MITM- атака на протокол
- CPC Ади Шамира

Составитель: Зав. кафедрой ИЗИ д.т.н., Монахов М.Ю.

должность, ФИО, подпись

Заведующий кафедрой ИЗИ М.Ю. Монахов

ФИО, подпись

Директор института ИТР А.А. Галкин

ФИО, подпись

Дата, Печать института (факультета)