АННОТАЦИЯ
дисциплины «ФТД.В.02 КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

**Объем трудоемкости:** 2 зачетные единицы (72 часа, из них – 24,2 часа контактной работы (12 часов лекций, 12 практических занятий, 0,2 часа ИКР); 47,8 часов самостоятельной работы).

**Цель дисциплины:**

Цель освоения дисциплины – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

**Задачи дисциплины:**

Задачи освоения дисциплины «Криптографические протоколы»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета и получение сведений:

о нормативных требованиях по административно-правовому регулированию в области криптографической защиты информации;

об основных задачах и понятиях криптографии;

об этапах развития криптографии;

о видах информации, подлежащей шифрованию;

о классификации шифров;

о методах криптографического синтеза и анализа;

о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;

о методах криптозащиты компьютерных систем и сетей.

**Место дисциплины в структуре ООП ВО**

Дисциплина «Криптографические протоколы» является факультативом.

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

**Требования к уровню освоения дисциплины**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

| № п.п. | Индекс компетенции | Содержание компетенции (или её части) | В результате изучения учебной дисциплины обучающиеся должны | | |
|---|---|---|---|---|---|
| | | | **знать** | **уметь** | **владеть** |
| 1. | ПК-4 | способность к применению методов математического и алгоритмического моделирования при решении теоретических и прикладных задач. | О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа. | Применять основные математические методы, используемые в анализе типовых алгоритмов. | использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений. |

**Основные разделы дисциплины:** Разделы дисциплины, изучаемые в 3 семестре

| № раздела | Наименование разделов | Количество часов | | | |
|---|---|---|---|---|---|
| | | Всего | Аудиторная работа | | Самостоятельная работа |
| | | | Л | Пр | |
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. | 18 | 2 | 4 | 12 |
| 2 | Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров. | 18 | 2 | 4 | 12 |
| 3 | Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами | 18 | 4 | 2 | 12 |
| 4 | Системы шифрования с открытыми ключами | 17,8 | 4 | 2 | 11,8 |
| | **Итого:** | | 12 | 12 | 47,8 |

**Курсовые работы**: не предусмотрены.
**Форма проведения аттестации по дисциплине:** зачет


1. Рябко Б.Я, Фионов А.Н. Основы современной криптографии и стеганографии, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2013. - URL: https://e.lanbook.com/book/63244
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: https://e.lanbook.com/book/70724


Автор РПД, д.ф.-м.н., профессор Рожков А.В.