АННОТАЦИЯ
дисциплины
Б.О.28 «КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

Направление подготовки/специальность

02.03.02 Фундаментальная информатика и информационные технологии

Курс 4 Семестры 8 Количество з.е. 3

Объем трудоемкости: 3 зачетных единицы (108 часов, из них – 48,3 часов контактной работы: лекционных 14 ч., лабораторных 28 ч., КСР 6 ч, ИКР 0,3 ч; 6 часов самостоятельной работы; 53,7 час. – на подготовку к экзамену).

Цель дисциплины:

Целью преподавания и изучения дисциплины «Дискретная математика» является формирование у студентов знаний и навыков по использованию методов согласованного решения задач информационного обмена с использованием криптографии.

Задачи дисциплины:

Студент должен знать основные алгорритмы, методы и средства криптографии; уметь применять теории, методы, алгоритмы криптографии; владеть знаниями теории, методов, алгоритмов построения криптографических протоколов для решения теоретических проблем фундаментальной информатики и практических задач информационных технологий.

Место дисциплины в структуре ООП ВО

Дисциплина «Криптографические протоколы» относится к профессиональной части обязательных дисциплин.

Для изучения дисциплины необходимо знания, полученные при изучении дисциплин дискретная математика, алгебра, методы программирования, основы теории вероятностей и статистических методов, компьютерные сети, конструирование алгоритмов и структур данных, программирование в компьютерных сетях, информационная безопасность. Знания, получаемые при изучении дисциплины Криптографические протоколы, используются при изучении магистерских дисциплин и служат основой для написания научно-исследовательской работы и выпускной квалификационной работы.

Результаты обучения (знания, умения, опыт, компетенции)

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций: ОПК-5 – Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности; ПК-1 – Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии

.

Основные разделы дисциплины

Криптографические протоколы и основные требования; Протоколы рукопожатия; Протоколы генерации ключей; Протоколы идентификации и аутентификации; Протоколы распределения ключей; Доказательства с нулевым разглашением секрета.

Курсовые работы

Не предусмотрены.

Вид аттестации

Экзамен в 8 семестре

Составитель:

Старший преподаватель кафедры ВТ ФКТиПМ Жук А.С.