Аннотация рабочей программы дисциплины «Криптографическая защита информации» для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.
специализация образовательной программы -

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины:

Дисциплина «Криптографическая защита информации» относится к дисциплинам профессионального цикла и является частью образовательной программы в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных системах.

Задачи изучения дисциплины:

2. Компетенции обучающегося, формируемые в результате освоения дисциплины и индикаторы их достижения

2.1. Профессиональные компетенции и индикаторы их достижения

Категория (группа) профессиональных компетенций	Код и наименование профессиональных компетенции	Минимальные требования
ПК 2.1.	ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей	ИД-1ПК 2.1 имеет практический опыт: установки, настройки, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС; ИД-2ПК 2.1 умеет: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить конфигурирование программных и программно- аппаратных (в том числе криптографических) средств защиты информации; ИД-3 ПК 2.1 знает: способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; типовые программные и программно-аппаратные средства защиты информации в ИТКС; криптографические средства защиты информации

		конфиденциального характера, которые применяются в ИТКС.
ПК 2.2.	ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	ИД-1ПК 2.2 имеет практический опыт: поддержания бесперебойной работы программных и программно- аппаратных (в том числе криптографических) средств защиты информации в ИТКС; ИД-2ПК 2.2 умеет: выявлять и оценивать угрозы безопасности информации в ИТКС; проводить контроль показателей и процесса функционирования программных и программно- аппаратных (в том числе криптографических) средств защиты информации; проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить техническое обслуживание и ремонт программно- аппаратных (в том числе криптографических) средств защиты информации; ИД-3ПК 2.2 знает: возможные угрозы безопасности информации в ИТКС; способов защиты информации от НСД и специальных воздействий на нее; порядок тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; организацию и содержание технического обслуживания и ремонта программно- аппаратных (в том числе криптографических) средств защиты информации; порядок и правила ведения эксплуатационной документации на программные и программно- аппаратные (в том числе криптографические) средства защиты информации.
ПК 2.3.	ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно–телекоммуникационных	ИД-1ПК 2.3 имеет практический опыт: защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно- аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями;

	системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	ИД-2ПК 2.3 умеет: выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно- аппаратных (в том числе криптографических) средств защиты информации; ИД-3ПК 2.3 знает: возможные угрозы безопасности информации в ИТКС; способов защиты информации НСД и специальных воздействий на нее; типовые программные и программно- аппаратные средства защиты информации в ИТКС; криптографические средств защиты информации конфиденциального характера, которые применяются в ИТКС; порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации

3. Содержание дисциплины

Введение в криптографию. Шифры замены и перестановки. Криптоанализ шифров замены и перестановки. Современные блочные шифры и их криптоанализ. Арифметика целых чисел. Криптография с ассиметричным ключом. Целостность, установление подлинности и управление ключами. Безопасность сети. Дифференцированный зачет.