Аннотация рабочей программы дисциплины «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты» для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.
специализация образовательной программы -

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины:

Программа междисциплинарного модуля МДК.02.01 Защита информации в информационно- телекоммуникационных системах и сетях с использованием программных и программно- аппаратных средств защиты является частью образовательной программы в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных системах.

Рабочая программа может быть использована в дополнительном профессиональном образовании.

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	Практический опыт: установки, настройки, испытаний и конфигурирования программных и программно- аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС; Умения: 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 Знания: способов защиты информации от несанкционированного доступа (далее – НСД) и специальных

		воздействий на нее; типовых программных и программно- аппаратных средств защиты информации в ИТКС; криптографических средств 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	Практический опыт: поддержания бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС Умения: 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 Знания: возможных угроз безопасности информации в ИТКС; способов защиты информации от НСД и специальных воздействий на нее; порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации; порядка и правил 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 системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	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 Умения: 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 Знания: возможных угроз безопасности информации в ИТКС; способов защиты информации НСД и специальных воздействий на нее; типовых программных и программно- аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации

3. Содержание дисциплины

Промежуточная аттестация. Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN. Тема 1.2. Технологии разграничения доступа. Тема 1.1. Обеспечение безопасности операционных систем.