

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Карпова Елизавета Александровна
Должность: директор
Дата подписания: 30.11.2023 16:19:57
Уникальный программный ключ:
ad9053b6a9e639199a21a41d1a80dd3f5c40650966caaf85dff11a7fd7d02cbad



СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
ЧАСТНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Криптографическая защита информации

Аннотация дисциплины (модуля)

Закреплена за кафедрой **Цикловая комиссия по информатике и информационной безопасности**
Учебный план 10.02.04 **ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Квалификация **Техник по защите информации**
Форма обучения **очная**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	5 (3.1)		6 (3.2)		Итого	
	УП	РП	УП	РП		
Неделя	13		6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	13	13	52	52	65	65
Практические	13	13	54	54	67	67
Итого ауд.	26	26	106	106	132	132
Контактная работа	26	26	106	106	132	132
Сам. работа	14	14	30	30	44	44
Итого	40	40	136	136	176	176

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	В результате изучения профессионального модуля студент должен освоить основной вид деятельности «Защита информации в информационно-телекоммуникационных системах
1.2	и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты» и соответствующие ему общие компетенции и
1.3	профессиональные компетенции:
1.4	<input type="checkbox"/> установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
1.5	<input type="checkbox"/> поддержании бесперебойной работы программных и программноаппаратных в том числе криптографических средств защиты информации в ИТКС;
1.6	<input type="checkbox"/> защите 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.
1.7	<input type="checkbox"/> выявлять и оценивать угрозы безопасности информации в ИТКС;
1.8	<input type="checkbox"/> настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
1.9	<input type="checkbox"/> проводить установку и настройку программных и программноаппаратных, в том числе криптографических средств защиты информации;
1.10	<input type="checkbox"/> проводить конфигурирование программных и программноаппаратных, в том числе криптографических средств защиты информации;
1.11	<input type="checkbox"/> проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
1.12	<input type="checkbox"/> проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
1.13	<input type="checkbox"/> проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации
1.14	<input type="checkbox"/> возможные угрозы безопасности информации в ИТКС;
1.15	<input type="checkbox"/> способы защиты информации от несанкционированного доступа(далее – НСД) и специальных воздействий на неё;
1.16	<input type="checkbox"/> типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
1.17	<input type="checkbox"/> криптографические средства защиты информации конфиденциального характера, которые применяются в информационнотелекоммуникационных системах и сетях;
1.18	<input type="checkbox"/> порядок тестирования функций программных и программноаппаратных, в том числе криптографических средств защиты информации;
1.19	<input type="checkbox"/> организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
1.20	<input type="checkbox"/> порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	МДК.02
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Организационное и правовое обеспечение информационной безопасности
2.1.2	Телекоммуникационные системы и сети
2.1.3	Учебная практика
2.1.4	Электроника и схемотехника
2.1.5	14601 "Монтажник оборудования связи"
2.1.6	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (для специальностей СПО)
2.1.7	Инженерная и компьютерная графика
2.1.8	Квалификационный экзамен
2.1.9	Основы алгоритмизации и программирования
2.1.10	Производственная практика
2.1.11	Учебная практика
2.1.12	Физика
2.1.13	Экономика и управление

2.1.14	Электротехника
2.1.15	Безопасность жизнедеятельности
2.1.16	Информатика
2.1.17	История
2.1.18	Математика
2.1.19	Основы информационной безопасности
2.1.20	Эксплуатация информационно-телекоммуникационных систем и сетей
2.1.21	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (для специальностей СПО)
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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 предъявляемыми требованиями.

Знать:

Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

Уметь:

Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

Владеть:

определения необходимых средств криптографической защиты информации;

ПК 2.2.: Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.

Знать:

типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;

Уметь:

особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах

Владеть:

пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации

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 оборудовании информационно-телекоммуникационных систем и сетей.

Знать:

типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;

Уметь:

выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;

Владеть:

определения необходимых средств криптографической защиты информации;

ОК 10.: Пользоваться профессиональной документацией на государственном и иностранном языках.

Знать:

основные понятия криптографии и типовые криптографические методы защиты информации;

Уметь:

производить установку и настройку типовых программно-аппаратных средств защиты информации;

Владеть:

определения необходимых средств криптографической защиты информации;

ОК 09.: Использовать информационные технологии в профессиональной деятельности.

Знать:

типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;

Уметь:
<input type="checkbox"/> производить установку и настройку типовых программно-аппаратных средств защиты информации;
Владеть:
<input type="checkbox"/> определения необходимых средств криптографической защиты информации;

ОК 04.: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
Знать:
<input type="checkbox"/> типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах
Уметь:
<input type="checkbox"/> выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах
Владеть:
<input type="checkbox"/> применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;

ОК 03.: Планировать и реализовывать собственное профессиональное и личностное развитие.
Знать:
возможные угрозы безопасности информации в ИТКС;
Уметь:
выявлять и оценивать угрозы безопасности информации в ИТКС
Владеть:
<input type="checkbox"/> определения необходимых средств криптографической защиты информации;

ОК 02.: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
Знать:
<input type="checkbox"/> основные понятия криптографии и типовые криптографические методы защиты информации;
Уметь:
<input type="checkbox"/> производить установку и настройку типовых программно-аппаратных средств защиты информации
Владеть:
<input type="checkbox"/> шифрования информации.

ОК 01.: Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
Знать:
<input type="checkbox"/> особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;
Уметь:
<input type="checkbox"/> пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
Владеть:
<input type="checkbox"/> применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;

В результате освоения дисциплины обучающийся должен

3.1	Знать:
	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
	<input type="checkbox"/> типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
	<input type="checkbox"/> типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
	<input type="checkbox"/> основные понятия криптографии и типовые криптографические методы защиты информации;
	<input type="checkbox"/> типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
	<input type="checkbox"/> типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах
	возможные угрозы безопасности информации в ИТКС;
	<input type="checkbox"/> основные понятия криптографии и типовые криптографические методы защиты информации;
	<input type="checkbox"/> особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;
3.2	Уметь:
	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

<input type="checkbox"/>	особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах
<input type="checkbox"/>	выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;
<input type="checkbox"/>	производить установку и настройку типовых программно-аппаратных средств защиты информации;
<input type="checkbox"/>	производить установку и настройку типовых программно-аппаратных средств защиты информации;
<input type="checkbox"/>	выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах
	выявлять и оценивать угрозы безопасности информации в ИТКС
<input type="checkbox"/>	производить установку и настройку типовых программно-аппаратных средств защиты информации
<input type="checkbox"/>	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
3.3	Владеть:
<input type="checkbox"/>	определения необходимых средств криптографической защиты информации;
<input type="checkbox"/>	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации
<input type="checkbox"/>	определения необходимых средств криптографической защиты информации;
<input type="checkbox"/>	определения необходимых средств криптографической защиты информации;
<input type="checkbox"/>	определения необходимых средств криптографической защиты информации;
<input type="checkbox"/>	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
<input type="checkbox"/>	определения необходимых средств криптографической защиты информации;
<input type="checkbox"/>	шифрования информации.
<input type="checkbox"/>	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;