

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Карпова Елизавета Александровна  
Должность: директор  
Дата подписания: 26.02.2022 19:51:05  
Уникальный программный ключ:  
ad9053b6a9e639199a21a41d1a80dd3f5c40650966aaf85dff11a7fd7d02cbad



**СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ**  
ЧАСТНОЕ УЧРЕЖДЕНИЕ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

## **Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты**

### **Аннотация дисциплины (модуля)**

Закреплена за кафедрой **Цикловая комиссия по информатике и информационной безопасности**

Учебный план Направление 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	16		6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	36	36	52	52
Практические	48	48	36	36	84	84
Итого ауд.	64	64	72	72	136	136
Контактная работа	64	64	72	72	136	136
Сам. работа	75	75	30	30	105	105
Итого	139	139	102	102	241	241

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Разработана в соответствии с ФГОС СПО специальности СПО 10.02.04
1.2	Обеспечение информационной безопасности телекоммуникационных систем
1.3	в части освоения основного вида деятельности: защита информации в
1.4	информационно-телекоммуникационных системах и сетях с использованием
1.5	программных и программно-аппаратных, в том числе криптографических
1.6	средств защиты и соответствующих профессиональных компетенций:
1.7	ПК 2.1. Производить установку, настройку, испытания и
1.8	конфигурирование программных и программно-аппаратных, в том числе
1.9	криптографических средств защиты информации от несанкционированного
1.10	доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетей.
1.11	ПК 2.2. Поддерживать бесперебойную работу программных и
1.12	программно-аппаратных, в том числе криптографических средств защиты
1.13	информации в информационно-телекоммуникационных системах и сетях.
1.14	ПК 2.3. Осуществлять защиту информации от несанкционированных
1.15	действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и
1.16	программно-аппаратных, в том числе криптографических средств в
1.17	соответствии с предъявляемыми требованиями.
1.18	Рабочая программа профессионального модуля может быть
1.19	использована в дополнительном профессиональном образовании.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	МДК.02
<b>2.1</b>	<b>Требования к предварительной подготовке обучающегося:</b>
2.1.1	Вычислительные системы, сети и телекоммуникации
2.1.2	Информационные системы и технологии
2.1.3	Теория вероятностей и математическая статистика
2.1.4	Экономика фирмы (предприятия)
2.1.5	Математика
2.1.6	Теория систем и системный анализ
2.1.7	Экономическая теория
2.1.8	Методы принятия управленческих решений
2.1.9	Студент в среде e-learning
2.1.10	Философия
2.1.11	Право
2.1.12	Современные ИКТ в образовании
<b>2.2</b>	<b>Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>
2.2.1	Проектный практикум
2.2.2	Производственная практика (технологическая (проектно-технологическая) практика)
2.2.3	Применение нейронных сетей в информационной сфере
2.2.4	Принципы построения нейрокомпьютеров
2.2.5	Подготовка к сдаче и сдача государственного экзамена

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
<b>ОК 01.: Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</b>	
<b>Знать:</b>	
<input type="checkbox"/> методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;	
<b>Уметь:</b>	
<input type="checkbox"/> типовые средства, методы и протоколы идентификации,	

аутентификации и авторизации;
<b>Владеть:</b>
диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности

**ОК 02.: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.**

<b>Знать:</b>
решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;
<b>Уметь:</b>
методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
<b>Владеть:</b>
типовые средства, методы и протоколы идентификации, аутентификации и авторизации;

**ОК 03.: Планировать и реализовывать собственное профессиональное и личностное развитие.**

<b>Знать:</b>
<input type="checkbox"/> типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
<b>Уметь:</b>
оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности
<b>Владеть:</b>
использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись

**ОК 04.: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.**

<b>Знать:</b>
особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
<b>Уметь:</b>
<input type="checkbox"/> применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно <input type="checkbox"/> аппаратными средствами.
<b>Владеть:</b>
применения программно-аппаратных средств обеспечения информационной безопасности;

**ОК 05.: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.**

<b>Знать:</b>
методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
<b>Уметь:</b>
применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно <input type="checkbox"/> аппаратными средствами
<b>Владеть:</b>
мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;

**ОК 09.: Использовать информационные технологии в профессиональной деятельности.**

<b>Знать:</b>
типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
<b>Уметь:</b>
оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
<b>Владеть:</b>
мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;

**ОК 10.: Пользоваться профессиональной документацией на государственном и иностранном языке.**

<b>Знать:</b>
решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
<b>Уметь:</b>
выполнять тестирование систем с целью определения уровня защищенности
<b>Владеть:</b>
- установки, настройки специализированного оборудования по защите 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.**

<b>Знать:</b>
- назначение, классификацию и принцип работы специализированного оборудования;
<b>Уметь:</b>
- выполнять тестирование систем с целью определения уровня защищенности
<b>Владеть:</b>
конфигурировании автоматизированных систем и информационно-коммуникационных сетей

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

<b>Знать:</b>
алгоритмы работы тестовых программ;
<b>Уметь:</b>
- применять криптографические методы защиты информации;
<b>Владеть:</b>
классифицировать угрозы информационной безопасности

**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.**

<b>Знать:</b>
- каналы утечки информации
<b>Уметь:</b>
выполнять тестирование систем с целью определения уровня защищенности;
<b>Владеть:</b>
- организации защиты в различных операционных системах и средах

**В результате освоения дисциплины обучающийся должен**

<b>3.1</b>	<b>Знать:</b>
<input type="checkbox"/>	методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
	решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;
<input type="checkbox"/>	типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
	особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
	методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
	типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
	решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
	- назначение, классификацию и принцип работы специализированного оборудования;
	алгоритмы работы тестовых программ;
	- каналы утечки информации
<b>3.2</b>	<b>Уметь:</b>
<input type="checkbox"/>	типовые средства, методы и протоколы идентификации, аутентификации и авторизации;

методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;	
оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности	
<input type="checkbox"/> применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно <input type="checkbox"/> аппаратными средствами.	
применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно <input type="checkbox"/> аппаратными средствами	
оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;	
выполнять тестирование систем с целью определения уровня защищенности	
- выполнять тестирование систем с целью определения уровня защищенности	
- применять криптографические методы защиты информации;	
выполнять тестирование систем с целью определения уровня защищенности;	
<b>3.3</b>	<b>Владеть:</b>
диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности	
типовые средства, методы и протоколы идентификации, аутентификации и авторизации;	
использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись	
применения программно-аппаратных средств обеспечения информационной безопасности;	
мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;	
мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;	
- установки, настройки специализированного оборудования по защите информации;	
конфигурировании автоматизированных систем и информационно-коммуникационных сетей	
классифицировать угрозы информационной безопасности	
- организации защиты в различных операционных системах и средах	