СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
ЧАСТНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«УТВЕРЖДАЮ»
Директор ЧУ ПО «СТК»
_____ Е. А. Карпова
27.01.2021 г.

Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

рабочая программа дисциплины (модуля)

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

Учебный план Направление 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Учебный год начала подготовки 2021-2022

Квалификация **Техник по защите информации**

Форма обучения **очная**

Часов по учебному плану 159
в том числе:
аудиторные занятия 133
самостоятельная работа 26

Виды контроля в семестрах:

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		**7 (4.1)**		Итого	
Недель	17		16			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	34	34	16	16	50	50
Практические	51	51	32	32	83	83
Итого ауд.	85	85	48	48	133	133
Контактная работа	85	85	48	48	133	133
Сам. работа	18	18	8	8	26	26
Итого	103	103	56	56	159	159

Рабочая программа дисциплины

Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (уровень подготовки кадров высшей квалификации). (приказ Минобрнауки России от 09.12.2016 г. № 1551)

составлена на основании учебного плана:

Направление 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

утвержденного на заседании Педагогического Совета ЧУ ПО "СТК" 24.01.2022 протокол № 1.

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 оборудование 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.03
2.1	**Требования к предварительной подготовке обучающегося:**
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
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
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)	
ОК 01.: Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	
Знать:	
1	□ методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
2	особенности применения программно-аппаратных средств

	обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
3	типовые модели управления доступом;
Уметь:	
1	□ типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
2	типовые средства и методы ведения аудита и обнаружение вторжений;
3	типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
Владеть:	
1	диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности
2	оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
3	участвовать в обеспечение учета, обработки, хранения и передачи конфиденциальной информации;

ОК 02.: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	
Знать:	
1	решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;
2	использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись
3	применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно□аппаратными средствами.
Уметь:	
1	методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
2	особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
3	типовые модели управления доступом;
Владеть:	
1	типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
2	типовые средства и методы ведения аудита и обнаружение вторжений;
3	□ типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;

ОК 03.: Планировать и реализовывать собственное профессиональное и личностное развитие.	
Знать:	
1	□ типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
2	основные понятия криптографии и типовые криптографические методы защиты информации
3	□ диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности
Уметь:	
1	оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности
2	участвовать в обеспечение учета, обработки, хранения и передачи конфиденциальной информации;
3	□ решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов
Владеть:	
1	использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись
2	применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно□аппаратными средствам

3	методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;

ОК 04.: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	
Знать:	
1	особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
2	типовые модели управления доступом;
3	типовые средства, методы и протоколы идентификации, аутентификации и авторизации
Уметь:	
1	применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно аппаратными средствами.
2	использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
3	решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;
Владеть:	
1	применения программно-аппаратных средств обеспечения информационной безопасности;
2	диагностики, устранение отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;
3	мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;

ОК 05.: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	
Знать:	
1	методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
2	особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
3	типовые модели управления доступом
Уметь:	
1	применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно аппаратными средствами
2	использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
3	решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;
Владеть:	
1	мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;
2	обеспечение учета, обработки, хранения и передачи конфиденциальной информации;
3	решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;

ОК 09.: Использовать информационные технологии в профессиональной деятельности.	
Знать:	
1	типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
2	основные понятия криптографии и типовые криптографические методы защиты информаци
3	типовые средства и методы ведения аудита и обнаружение вторжений;
Уметь:	
1	оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
2	участвовать в обеспечение учета, обработки, хранения и передачи конфиденциальной информации;
3	решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов
Владеть:	
1	мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;

2	обеспечение учета, обработки, хранения и передачи конфиденциальной информации;
3	решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;

ОК 10.: Пользоваться профессиональной документацией на государственном и иностранном языке.	
Знать:	
1	решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
2	- каналы утечки информации
3	- назначение, классификацию и принцип работы специализированного оборудования
Уметь:	
1	выполнять тестирование систем с целью определения уровня защищенности
2	- использовать программные продукты для защиты баз данных;
3	применять криптографические методы защиты информации;
Владеть:	
1	- установки, настройки специализированного оборудования по защите информации;
2	- выделения возможных атак на автоматизированные системы;
3	установки и настройке программных средств защиты автоматизированных систем и информационно□коммуникационных сетей;

ПК 3.1.: Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.	
Знать:	
1	оценивать точность проводимых измерений;
2	- оформлять эксплуатационную и ремонтную документацию;
3	- принципы построения информационно-телекоммуникационных систем и сетей;
Уметь:	
1	- базовые технологии построения и состав оборудования мультисервисных сетей связи
2	- состав и основные характеристики типового оборудования ИТКС
3	- принципы передачи информации в ИТКС;
Владеть:	
1	- принципы передачи информации в ИТКС;
2	- принципы помехоустойчивого кодирования сигналов ИТКС;
3	виды и характеристики сигналов в ИТКС;

ПК 3.2.: Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.	
Знать:	
1	- принципы аналого-цифрового преобразования, работы компандера, коде□ра и декодера;
2	особенности распространения электромагнитных волн различных диапазонов частот;
3	- виды помех в каналах связи, методы защиты от них
Уметь:	
1	разновидности проводных линий передачи;
2	- конструкцию и характеристики электрических и оптических кабелей связи;
3	- способы коммутации в сетях связи
Владеть:	
1	принципы построения многоканальных систем передачи;
2	принципы построения радиолиний и систем радиосвязи;
3	- основы маршрутизации в информационно-телекоммуникационных сетях

ПК 3.3.: Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
Знать:

1	принципы построения, основные характеристики и оборудование систем подвижной радиосвязи;
2	технологии и оборудование удаленного доступа в информационно□телекоммуникационных сетях;
3	типовые услуги, предоставляемые с использованием информационно□телекоммуникационных сетей, виды информационного обслуживания, предо□ставляемые пользователям
Уметь:	
1	принципы построения и технические средства локальных сетей;
2	принципы функционирования маршрутизаторов;
3	модемы, использующиеся в ИТКС, принципы подключения и функционирова□ния;
Владеть:	
1	- спецификацию изделий, комплектующих, запасного имущества и ремонт□ных материалов, порядок их учета и хранени
2	принципы организации эксплуатации ИТКС;
3	содержание технического обслуживания и восстановления работоспособ□ности оборудования ИТ

ПК 3.4.: Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.	
Знать:	
1	- принципы организации и технологию ремонта оборудования ИТКС
2	- периодичность поверок контрольно-измерительной аппаратуры;
3	принцип действия выпрямителей переменного тока
Уметь:	
1	принципы работы стабилизаторов напряжения и тока, импульсных источ□ников питания.
2	- принципы защиты электронных устройств от недопустимых режимов работы;
3	принципы построения, основные характеристики типовых измерительных приборов и правила работы с ними;
Владеть:	
1	основные понятия и определения метрологии, стандартизации и сертифи□кации.
2	оформлять эксплуатационную и ремонтную документацию;
3	осуществлять настройку модемов, используемых в защищенных теле□коммуникационных системах;

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	□ методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
3.1.2	□ особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
3.1.3	□ типовые модели управления доступом;
3.1.4	□ типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
3.1.5	□ типовые средства и методы ведения аудита и обнаружение
3.1.6	вторжений;
3.1.7	□ типовые средства и методы обеспечения информационной
3.1.8	безопасности в локальных и глобальных вычислительных сетях;
3.1.9	□ основные понятия криптографии и типовые криптографические
3.1.10	методы защиты информаци
3.2	**Уметь:**
3.2.1	применять программно-аппаратные средства обеспечения информационной безопасности;
3.2.2	□ диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
3.2.3	□ оценивать эффективность применяемых программно-аппаратных
3.2.4	средств обеспечения информационной безопасности;
3.2.5	□ участвовать в обеспечение учета, обработки, хранения и передачи
3.2.6	конфиденциальной информации;
3.2.7	□ решать частые технические задачи, возникающие при аттестации
3.2.8	объектов, помещений, программ, алгоритмов;
3.2.9	□ использовать типовые криптографические средства и методы защиты

3.2.10	информации, в том числе и электронную цифровую подпись;
3.2.11	□ применять нормативные правовые акты, нормативные методические
3.2.12	документы по обеспечению информационной безопасности программно□аппаратными средствами.
3.3	**Владеть:**
3.3.1	□ применения программно-аппаратных средств обеспечения информационной безопасности;
3.3.2	□ диагностики, устранение отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;
3.3.3	□ мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;
3.3.4	□ обеспечение учета, обработки, хранения и передачи конфиденциальной информации;
3.3.5	□ решение частных технических задач, возникающих при аттестации
3.3.6	объектов, помещений, программ, алгоритмов;
3.3.7	□ применение нормативных правовых актов, нормативных
3.3.8	методических документов по обеспечению информационной безопасности
3.3.9	программно-аппаратными средствами.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов
	Раздел 1.		
1.1	Предмет и задачи программноаппаратной защиты нформации Предмет и задачи программно-аппаратной защиты информации Основные понятия программно-аппаратной защиты информации Классификация методов и средств программно-аппаратной защиты информации /Лек/	6	20
1.2	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов /Пр/	6	22
1.3	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. /Ср/	6	14
	Раздел 2.		
2.1	Автоматизация процесса обработки информации Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении.Основные виды АС в защищенном исполнении.Методы создания безопасных систем Методология проектирования гарантированно защищенных КС Дискреционные модели. Мандатные модели /Лек/	6	1
2.2	Учет, обработка, хранение и передача информации в АИС.Ограничение доступа на вход в систему.Идентификация и аутентификация пользователей. Разграничение доступа. Регистрация событий (аудит).Контроль целостности данных /Пр/	6	1
2.3	Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности. Криптографическая защита. Обзор программ шифрования данных.Управление политикой безопасности. Шаблоны безопасности /Ср/	6	1
	Раздел 3.		
3.1	Источники дестабилизирующего воздействия на объекты защиты.Способы воздействия на информацию.Причины и условия дестабилизирующего воздействия на информацию /Лек/	6	11
3.2	Распределение каналов в соответствии с источниками воздействия на информацию /Пр/	6	26
3.3	Распределение каналов в соответствии с источниками воздействия на информацию /Ср/	6	1

	Раздел 4.		
4.1	Понятие несанкционированного доступа к информации.Основные подходы к защите информации от НСД.Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.Доступ к данным со стороны процесса.Особенности защиты данных от изменения. Шифрование. /Лек/	6	1
4.2	Организация доступа к файлам.Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД /Пр/	6	1
4.3	Организация доступа к файлам.Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД /Ср/	6	1
4.4	Работа автономной АС в защищенном режиме Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка) Применение закладок, направленных на снижение эффективности средств, замыкающих среду. /Лек/	6	1
4.5	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО /Пр/	6	1
4.6	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО /Ср/	6	1
4.7	Вредоносное программное обеспечение как особый вид разрушающих воздействий Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. Бот-неты. Принцип функционирования. Методы обнаружения Классификация антивирусных средств. Сигнатурный и эвристический анализ Защита от вирусов в "ручном режиме" Основные концепции построения систем антивирусной защиты на предприятии /Лек/	7	10
4.8	Несанкционированное копирование программ как тип НСД Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Привязка ПО к аппаратному окружению и носителям.Защитные механизмы в современном программном обеспечении на примере MS Offic /Пр/	7	10
4.9	Защита информации от несанкционированного копирования с использованием специализированных программных средств Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) /Ср/	7	5
4.10	Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов.Безвозвратное удаление данных. Принципы и алгоритмы /Лек/	7	5
4.11	Применение средства восстановления остаточной информации на примере Foremost или аналога. Применение специализированного программно средства для восстановления удаленных файлов.Применение программ для безвозвратного удаления данных. Применение программ для шифрования данных на съемных носителях /Пр/	7	11
4.12	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ Устройства Touch Memory /Ср/	7	2

4.13	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ вторжений Использование сетевых снифферов в качестве СОВ Аппаратный компонент СОВ Программный компонент СОВ Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений. /Лек/	7	1
4.14	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений /Пр/	7	11
4.15	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом. /Ср/	7	1

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Вопросы для самоконтроля и текущей аттестации

Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах
Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности
Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности
Составление документации по учету, обработке, хранению и передаче конфиденциальной информации
Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации
Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.
Устранение замечаний по результатам проверки
Анализ и составление нормативных методических документов по обеспечению информационной безопасности программноаппаратными средствами, с учетом нормативных правовых актов.
Применение математических методов для оценки качества и выбора наилучшего программного средствахитектура предприятия?
На какие вопросы отвечает модель архитектуры предприятия?
Из каких этапов состоит цикл разработки архитектуры?
Для чего предназначены процессы соответствия?
Чем отличаются определения процесса различных школ?
Что такое документирование процесса?
Как классифицируются процессы?
В чем состоит цикл управления процессами?
Каковы основные понятия системного анализа?
Перечислите основные методологии описания деятельности.
Что такое бизнес-инжиниринг?
Расскажите об особенностях инструментальной системы ARIS.
Расскажите об особенностях инструментальной системы BPWin.
Расскажите об особенностях инструментальной системы Rational Rose.
Расскажите об особенностях графического редактора Visio.
Назовите основные принципы выделения бизнес-процессов.

5.2. Темы письменных работ (контрольных и курсовых работ, рефератов)

Темы курсовых проектов
ПроИстория развития криптографии
Программная реализация классических шифров
Оптимизация методов частотного анализа моноалфавитных шифров.
Программная реализация классических шифров
Методы механизации шифрования
Цифровое представление различных форм информации
Анализ современных симметричных криптоалгоритмов
Анализ современных асимметричных криптоалгоритмов
Программная реализация современных криптоалгоритмов
Сравнительный анализ функций хеширования
Аутентификация сообщений
Законодательство в области криптографической защиты информации
Перспективные направления криптографии

5.3. Оценочные средства для промежуточной аттестации

2. Составление таблиц классификации по темам
3. Составление протокола проверок объекта защиты в соответствии с требованиями информационной безопасности.
4. Проведение аттестации объекта защиты по вариантам
5. Конфигурирование комплексной системы защиты информаци

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год, эл. адрес
Л1.1	Фергюсон Н.	Практическая криптография	, 2005
Л1.2	Золотов С. Ю.	Проектирование информационных систем: учебное пособие: Учебники и учебные пособия для ВУЗов	Томск: Эль Контент, 2013 http://biblioclub.ru/index.php?page=book&id=208706&sr=1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год, эл. адрес
Л2.1	Левин М.	Криптография без секретов. Руководство пользователя	М.: Новый издательский дом, 2005
Л2.2	Платёнкин А.В., Рак И.П., Терехов А.В., Чернышов В.Н.	Проектирование информационных систем. Проектный практикум: Учебники и учебные пособия для ВУЗов	Тамбовский государственный технический университет (ТГТУ), 2015 https://biblioclub.ru/index.php?page=book_red&id=444966&sr=1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

6.2.1 Перечень программного обеспечения

6.3.1.1	Micorosft Windows, OpenOffice, доступ в сеть Интернет, Ramus educational 1.2.5

6.2.2 Перечень информационных справочных систем и ресурсов сети Интернет

6.3.2.1	https://github.com/ Веб-сервис для хостинга ИТ-проектов и их совместной разработки
6.3.2.2	ГОСТ Р 57193-2016 — Системная и программная инженерия. Процессы жизненного цикла систем. Дата введения 2017-11-01. URL: https://docs.cntd.ru/document/1200141163 (дата обращения: 14.04.2021). – Текст: электронный.
6.3.2.3	http://www.consultant.ru/ Справочная правовая система «КонсультантПлюс».
6.3.2.4	sdo.tiei.ru - Электронная информационно-образовательная среда(ЭИОС)
6.3.2.5	http://biblioclub.ru/ ЭБС «Университетская библиотека online»
6.3.2.6	http://library.tiei.ru/ - ЭЛЕКТРОННАЯ НАУЧНО-ОБРАЗОВАТЕЛЬНАЯ БИБЛИОТЕКА
6.3.2.7	https://www.intuit.ru/studies/courses/2195/55/info - Проектирование ИС. Интуит
6.3.2.8	https://www.sciencedirect.com/ Электронные журналы издательства Elsevier, Информатика и информационные технологии
6.3.2.9	https://habr.com/ru/ Коллективный блог публикаций, связанных с информационными технологиями,
6.3.2.10	https://github.com/ Веб-сервис для хостинга ИТ-проектов и их совместной разработки
6.3.2.11	http://n-t.ru/ База книг и публикаций Электронной библиотеки «Наука и техника»

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей). Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно - образовательную среду.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.

Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание -обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.
Главная задача лекционного курса - сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.
Основные функции лекций: 1. Познавательно-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. информационная.
Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.
Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.
При подготовке важны не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.
При проведении учебных занятий обеспечиваются развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).
Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.
Для контроля знаний студентов по данной дисциплине необходимо проводить оперативный, рубежный и итоговый контроль.
Оперативный контроль осуществляется путем проведения опросов студентов на семинарских занятиях, проверки выполнения практических заданий, а также учета вовлеченности (активности) студентов при обсуждении мини-докладов, организации ролевых игр и т.п.
Контроль за самостоятельной работой студентов по курсу осуществляется в двух формах: текущий контроль и итоговый.
Рубежный контроль (аттестация) подразумевает проведение тестирования по пройденным разделам курса. В тестирование могут быть включены темы, предложенные студентам для самостоятельной подготовки, а также практические задания.