СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
ЧАСТНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«УТВЕРЖДАЮ»
Директор ЧУ ПО «СТК»
_____ Е. А. Карпова
27.01.2020 г.

Криптографическая защита информации

рабочая программа дисциплины (модуля)

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

Учебный план 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Учебный год начала подготовки 2020-2021

Квалификация **Техник по защите информации**

Форма обучения **очная**

Часов по учебному плану 236
в том числе:
аудиторные занятия 168
самостоятельная работа 68

Виды контроля в семестрах:

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		**8 (4.2)**		Итого	
Недель	13		6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	13	13	70	70	83	83
Практические	13	13	72	72	85	85
Итого ауд.	26	26	142	142	168	168
Контактная работа	26	26	142	142	168	168
Сам. работа	14	14	54	54	68	68
Итого	40	40	196	196	236	236

Рабочая программа дисциплины

Криптографическая защита информации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ (приказ Минобрнауки России от 09.12.2016 г. № 1551)

составлена на основании учебного плана:

10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

утвержденного на заседании Педагогического Совета ЧУ ПО "СТК" 26.02.2021 протокол № 3.

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	установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
1.5	поддержании бесперебойной работы программных и программноаппаратных в том числе криптографических средств защиты информации в ИТКС;
1.6	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	выявлять и оценивать угрозы безопасности информации в ИТКС;
1.8	настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
1.9	проводить установку и настройку программных и программноаппаратных, в том числе криптографических средств защиты информации;
1.10	проводить конфигурирование программных и программноаппаратных, в том числе криптографических средств защиты информации;
1.11	проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
1.12	проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
1.13	проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации
1.14	возможные угрозы безопасности информации в ИТКС;
1.15	способы защиты информации от несанкционированного доступа(далее – НСД) и специальных воздействий на неё;
1.16	типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
1.17	криптографические средства защиты информации конфиденциального характера, которые применяются в информационнотелекоммуникационных системах и сетях;
1.18	порядок тестирования функций программных и программноаппаратных, в том числе криптографических средств защиты информации;
1.19	организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
1.20	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:	
1	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
3	Планировать и реализовывать собственное профессиональное и личностное развитие.
Уметь:	
1	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
2	Использовать информационные технологии в профессиональной деятельности.
3	Пользоваться профессиональной документацией на государственном и иностранном языке
Владеть:	
1	определения необходимых средств криптографической защиты информации;
2	использования программно-аппаратных криптографических средств защиты информации;
3	установки, настройки специализированного оборудования 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:	
1	типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
2	основные протоколы идентификации и аутентификации в телекоммуникационных системах;
3	состав и возможности типовых конфигураций программно-аппаратных средств защиты информации
Уметь:	
1	особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах
2	основные способы противодействия
3	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;
Владеть:	
1	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации
2	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
3	шифрования 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 оборудование информационно-телекоммуникационных систем и сетей.	
Знать:	
1	типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных

	системах;
2	□ основные протоколы идентификации и аутентификации в телекоммуникационных системах;
3	□ состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;
Уметь:	
1	□ выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;
2	□ определять рациональные методы и средства защиты на объектах и оценивать их эффективность
3	□ производить установку и настройку типовых программно-аппаратных средств защиты информации;
Владеть:	
1	□ определения необходимых средств криптографической защиты информации;
2	□ использования программно-аппаратных криптографических средств защиты информации;
3	□ установки, настройки специализированного оборудования криптографической защиты информации;

ОК 10.: Пользоваться профессиональной документацией на государственном и иностранном языках.	
Знать:	
1	□ основные понятия криптографии и типовые криптографические методы защиты информации;
2	□ несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы
3	□ основные способы противодействия
Уметь:	
1	□ производить установку и настройку типовых программно-аппаратных средств защиты информации;
2	□ определять рациональные методы и средства защиты на объектах и оценивать их эффективность
3	□ пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации
Владеть:	
1	□ определения необходимых средств криптографической защиты информации;
2	□ использования программно-аппаратных криптографических средств защиты информации;
3	□ применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем

ОК 09.: Использовать информационные технологии в профессиональной деятельности.	
Знать:	
1	□ типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
2	□ основные протоколы идентификации и аутентификации в телекоммуникационных системах;
3	□ состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;
Уметь:	
1	□ производить установку и настройку типовых программно-аппаратных средств защиты информации;
2	□ пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
3	□ выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах
Владеть:	
1	□ определения необходимых средств криптографической защиты информации;
2	□ использования программно-аппаратных криптографических средств защиты информации;
3	установки, настройки специализированного оборудования криптографической защиты информации;

ОК 04.: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	
Знать:	
1	□ типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах
2	□ основные протоколы идентификации и аутентификации в телекоммуникационных системах;
3	□ состав и возможности типовых конфигураций программно-аппаратных средств защиты

	информации
Уметь:	
1	выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах
2	определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
3	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
Владеть:	
1	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
2	шифрования информации
3	установки, настройки специализированного оборудования криптографической защиты информации

ОК 03.: Планировать и реализовывать собственное профессиональное и личностное развитие.	
Знать:	
1	возможные угрозы безопасности информации в ИТКС;
2	способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё
3	типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
Уметь:	
1	выявлять и оценивать угрозы безопасности информации в ИТКС
2	проводить конфигурирование программных и программноаппаратных, в том числе криптографических средств защиты информации
3	проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации
Владеть:	
1	определения необходимых средств криптографической защиты информации;
2	использования программно-аппаратных криптографических средств защиты информации;
3	установки, настройки специализированного оборудования криптографической защиты информации

ОК 02.: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	
Знать:	
1	основные понятия криптографии и типовые криптографические методы защиты информации;
2	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;
3	основные способы противодействия
Уметь:	
1	производить установку и настройку типовых программно-аппаратных средств защиты
2	определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
3	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации
Владеть:	
1	шифрования информации.
2	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
3	установки, настройки специализированного оборудования криптографической защиты информации

ОК 01.: Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	
Знать:	
1	особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;
2	основные способы противодействия
3	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы

Уметь:	
1	□ пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
2	□ производить установку и настройку типовых программно-аппаратных средств защиты информации;
3	□ определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
Владеть:	
1	□ применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
2	□ шифрования информации.
3	□ определения необходимых средств криптографической защиты информации;

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	□ возможные угрозы безопасности информации в ИТКС;
3.1.2	□ способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
3.1.3	□ типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
3.1.4	□ криптографические средства защиты информации конфиденциального характера, которые применяются в информационнотелекоммуникационных системах и сетях;
3.1.5	□ порядок тестирования функций программных и программноаппаратных, в том числе криптографических средств защиты информации;
3.1.6	□ организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
3.1.7	□ порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации
3.2	**Уметь:**
3.2.1	□ выявлять и оценивать угрозы безопасности информации в ИТКС;
3.2.2	□ настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
3.2.3	□ проводить установку и настройку программных и программноаппаратных, в том числе криптографических средств защиты информации;
3.2.4	□ проводить конфигурирование программных и программноаппаратных, в том числе криптографических средств защиты информации;
3.2.5	□ проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
3.2.6	□ проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
3.2.7	□ проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации
3.3	**Владеть:**
3.3.1	□ установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
3.3.2	□ поддержании бесперебойной работы программных и программноаппаратных в том числе криптографических средств защиты информации в ИТКС;
3.3.3	□ защите информации от НСД и специальных воздействий в ИТКС с
3.3.4	использованием программных и программно-аппаратных в том числе
3.3.5	криптографических средств защиты в соответствии с предъявляемыми
3.3.6	требованиями

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**
	Раздел 1.		

1.1	Обеспечение безопасности операционных систем Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows XP. Windows 7. Windows8. Linux. QNX и другие операционные системы. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации. Пароли. PIN-коды. Методы надежного составления паролей. Строгая аутентификация. Односторонняя аутентификация. Двухсторонняя аутентификация Аппаратно-программные средства идентификации и аутентификации. Токены. Смарт-карты. Виртуальные ключи. Программно-аппаратные модули доверенной загрузки. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. АПМДЗ Криптон –Замок системный администратор. Изучение настроек системного администратора АПМДЗ. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ Сектор НЖМД. Область памяти. Файл, папка, каталог. /Лек/	7	4
1.2	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав пользователя Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита Настройка изолированной среды АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование Восстановление информации типовыми средствами Программы восстановление информации /Пр/	7	4
1.3	Восстановление информации типовыми средствами Программы восстановление информации /Ср/	7	4
1.4	Технологии разграничения доступаАрхитектура подсистемы защиты операционной системы Windows Server2016. Особенности ОС Windows Server2016. Возможности администратора. Разграничение доступа к объектам операционной системы. Модели доступа. Дискреционная модель. Мандатная модель. Роли. Локальная политика безопасности. Настройка локальной политики безопасности. Администрирование системы. Изолированная программная среда. Способы организации. Методы применения. ActiveDirectory. Комплексная система организации управления доступом. Инсталяция. Настройка. Аудит безопасности операционной системы. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. Особенности функционирования межсетевых экранов. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Схемы защиты на базе межсетевых экранов. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. /Лек/	7	4
1.5	Программы надежного удаления информации Архивирование информации Программные средства резервного копирования. Настройка RAID-массивов Инсайдерская информация. Программы сбора информации о ПК Настройка межсетевого экрана /Пр/	7	4
1.6	Программы сбора информации о ПК Настройка межсетевого экрана /Ср/	7	4

1.7	Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN.Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP. Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. VPN – решения для построения защищенных сетей. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. протоколы SSL, TLS, SOCKS. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом. Web-доступ. Протоколы PAP, CHAP, S/Key, SSO, Kerberos. /Лек/	7	3
1.8	Основные действия с виртуальной машиной Работа с контрольными точками Использование внешних устройств Работа с локальным хранилищем сертификатов в ОС WINDOWS Установка и настройка ПО eTokenPKIClient Настройка ПО eTokenPKIClient с помощью групповых политик Развертывание TMS в среде Active Directory Настройка TMS в среде Active Directory Настройка политик TMS Настройка использования виртуального токена Использование токена на рабочем месте администратора Установка и настройка СКЗИ «КриптоПроCSP» Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP Применение SecretDisk4 Применение SecretDisk Server NG Изучение основных возможностей ПО VipNetClient Изучение настроек ПО VipNetClient Изучение возможностей ПО Деловая почта /Пр/	7	3
1.9	Изучение основных возможностей ПО /Ср/	7	4
1.10	Технологии обнаружения вторжений. Технология обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак. Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ. /Лек/	7	2
1.11	Изучение средств обнаружения атак Изучение антивирусных продуктов /Пр/	7	2
1.12	Изучение средств обнаружения атак Изучение антивирусных продуктов /Ср/	7	2
1.13	Методы управления средствами защиты.Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. Обзор современных систем управления сетевой защитой. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты. /Лек/	8	10
1.14	Пароли. PIN-коды. Методы надежного составления паролей. 5.Токены. Смарт-карты. Виртуальные ключи. 6.Программно-аппаратные модули доверенной загрузки. 7.АПМДЗ Криптон –Замок системный администратор. 8.Изучение настроек системного администратора АПМДЗ. /Пр/	8	15

1.15	9.Сектор НЖМД. Область памяти. Файл, папка, каталог. 10.Разграничение доступа к объектам операционной системы. 11.Комплексная система организации управления доступом. Инсталяция. Настройка. 12.Аудит безопасности операционной системы. 13.Функции межсетевых экранов.Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. /Ср/	8	14
1.16	Основы криптографических методов защиты информации.Свойства информационной безопасности. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности. Криптографические методы. Шифрование. Кодирование. Стеганография. Сжатие. Математика криптографии. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Традиционные шифры перестановки. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. Традиционные шифры замены. Шифры замены. Шифры многоалфавитной замены. Частотность символов. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей. /Лек/	8	20
1.17	Стеганографические методы скрытия информации Бинарная арифметика. Модульная арифметика Применение методов шифрования перестановкой Применение методов шифрования заменой Применение методов шифрования многоалфавитной замены Криптоанализ методов перестановки Криптоанализ методов замены Компьютерное шифрование /Пр/	8	20
1.18	Криптоанализ методов перестановки Криптоанализ методов замены Компьютерное шифрование /Ср/	8	10
1.19	Современные стандарты шифрования. Симметричное шифрование. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES. Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES. Российские стандарты симметричного шифрования. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. Проблема распределения ключей симметричного шифрования. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. Асимметричное шифрование. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль -Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП. Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов /Лек/	8	20
1.20	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители /Пр/	8	20
1.21	Алгоритм разложения произведения двух простых чисел на множители /Ср/	8	15

1.22	Криптографические методы обеспечения безопасности сетевых технологий. Целостность сообщения. Случайная модель Огас1е. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции. Электронная цифровая подпись. Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012. Установление подлинности объекта. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. Проблемы распределения открытого ключа асимметричного шифрования. Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. Электронная почта. Архитектура e-mail. PGP. S/M1ME. Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети Защита информации в сетях, организованных по технологии беспроводного доступа. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16. Защита информации в сетях сотовой связи. A3. A8.A5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи. Криптовалюты. Биткоин. Блокчейн-системы Ethereum. Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов. /Лек/	8	20
1.23	Разработка хэш-функции Разработка схемы простого пароля Разработка схемы динамического пароля Сертификаты открытого ключа Настройка и администрирование токена Настройка сервисов Рутокен-PinPad Настройка сервисов Рутокен-ЭЦП Настройка сервисов Рутокен–Bluetooth Настройка сервисов Рутокен–S Разработка алгоритма PGP Изучение протоколов SSL, TLS, IPSec Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2 /Пр/	8	17
1.24	1. Изучение новых технологий хранения информации. 2. Статистика и анализ крупных утечек информации за год. 3. Поиск информации о новых видах атак на информационную систему. 4. Обзор современных программных и программно-аппаратных средств защиты. 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты. 6. Криптографические методы.	8	15

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Вопросы для самоконтроля и текущей аттестации

1. Модель угроз НСД на предприятии
2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии
3. Проведение классификации ПО по требованиям ФСТЭК на предприятии
4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии
5. Построение модели нарушителя по требованиям ФСТЭК на предприятии
6. Построение модели нарушителя по требованиям ФСБ на предприятии
7. Модель угроз безопасности ИС персональных данных на предприятии
8. Комплексная модель защиты информации на предприятии.
9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
13. Проблема защиты информации в облачных хранилищах данных и ЦОДах
14. Защита сред виртуализации.

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

Проблемы обеспечения безопасности операционных систем.

2. Технологии аутентификации.
3. Аутентификация, авторизация и администрирование действий пользователя.
4. Пароли.
5. PIN-коды.
6. Методы надежного составления паролей.
7. Токены.
8. Смарт-карты.
9. Виртуальные ключи.
10. Программно-аппаратные модули доверенной загрузки.
11. АПМДЗ Криптон –Замок системный администратор.
12. Изучение настроек системного администратора АПМДЗ.
13. Сектор НЖМД.
14. Область памяти.
15. Файл, папка, каталог.
16. Разграничение доступа к объектам операционной системы.
17. Комплексная система организации управления доступом.
18. Инсталляция. Настройка.
19. Аудит безопасности операционной системы.
20. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика.
52
20
21. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.
22. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ.
23. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.
24. Концепция построения виртуальных защищенных сетей;.
25. Виртуальные защищенные сети.
26. Туннелирование.
27. Инкапсуляция пакетов.
28. Структура защищенного пакета.
29. Варианты построения защищенных каналов.
30. Защита на канальном уровне.
31. ПротоколыPPTP, L2F, L2TP.
32. Протоколы формирования защищенных каналов на сеансовом уровне.
33. Протоколы SSL, TLS, SOCKS.
34. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP.
35. Защита на прикладном уровне.
36. Протоколы PAP, CHAP, S/Key, SSO, Kerberos.
38. Функционирование системы управления средствами защиты.
39. Аудит безопасности информационной системы.

5.3. Оценочные средства для промежуточной аттестации

Введение. Выдача заданий
2 Анализ поставленной задачи
3 Определение защищаемых информационных активов. Категорирование информации
4 Определение уязвимостей и угроз
5 Анализ и выбор возможных решений по защите
6 Анализ механизмов защиты
7 Анализ требуемых компонентов
8 Проектирование модели угроз
9 Настройка компонентов защиты
10 Конфигурирование пользовательских задач
11 Проектирование эксперимента по внедрению системы защиты
12 Нормативно-правовое обеспечение проекта
13 Расчет индекса ROSI
14 Подготовка пояснительной записки к курсовому проекту
15 Защита курсового проекта

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

6.1. Рекомендуемая литература

6.2.1 Перечень программного обеспечения

6.3.1.1	Open Office

6.2.2 Перечень информационных справочных систем и ресурсов сети Интернет	
6.3.2.1	http://www.consultant.ru/ Справочная правовая система «КонсультантПлюс».
6.3.2.2	http://biblioclub.ru/ ЭБС «Университетская библиотека online»
6.3.2.3	http://library.tiei.ru/ - ЭЛЕКТРОННАЯ НАУЧНО-ОБРАЗОВАТЕЛЬНАЯ БИБЛИОТЕКА

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа,
7.2	занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и
7.3	индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для
7.4	самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования.
7.5	Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения,
7.6	служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного
7.7	типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие
7.8	тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным
7.9	программам дисциплин (модулей). Помещения для самостоятельной работы обучающихся оснащены
7.10	компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную
7.11	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 стр. 16

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