Федеральное агентство связи
Колледж телекоммуникаций
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Согласовано:
Генеральный директор
Андрианова Светлана Сергеевна
ООО «Аудиторы корпоративной безопасности»
_____ / Андрианова С.С. /
«__» _____ 2020 г.

УТВЕРЖДЕНО
приказом директора КТ МТУСИ
№ 01-03-113/1 от «19» июня 2020
_____ С.Н. Ильиных

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ, В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

для специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(очная форма обучения)

Москва, 2020 г.

ОДОБРЕНА
предметной (цикловой) комиссией
Компьютерных систем и безопасности
наименование комиссии

Протокол № 5
от «09» июня 2020 г.

Председатель предметной (цикловой) комиссии

_____ / Сергеева М.Б/

Разработано на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (приказ Минобрнауки России № 1551 от 09 декабря 2016 года) и примерной основной образовательной программы 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем. Зарегистрировано в государственном реестре примерных основных образовательных программ. Реквизиты решения ФУМО о включении ПООП в реестр: Протокол № 1 от 28.03.2017

Рассмотрено и одобрено на заседании методического совета
«10» июня 2020 г. Протокол № 5

СОГЛАСОВАНА:
Начальник методического отдела

_____ / Л.М.Кузнецова/
Подпись Ф.И.О.

Организация-разработчик:
КТ МТУСИ, Г. Москва

Разработчик:
Преподаватель КТМТУСИ: Сергеева М.Б.

Содержание программы реализуется в процессе освоения студентами основной профессиональной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в соответствии с требованиями ФГОС СПО для очной формы обучения.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является частью образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части освоения основного вида деятельности (ВД): **Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты** и соответствующих профессиональных компетенций (ПК):

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;

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

ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации в соответствии с предъявляемыми требованиями.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и в профессиональной подготовке, в программах повышения квалификации и переподготовки по должностям служащих. Рабочая программа профессионального модуля может быть использована на очной и очно-заочной формах обучения.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

Умения	Знания	Практический опыт
выявлять и оценивать угрозы безопасности информации в ИТКС; выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить восстановление процесса и параметров функционирования программных и программно-аппаратных	возможных угроз безопасности информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации;	защита 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; поддержание бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС; установка, настройка,

(в том числе криптографических) средств защиты информации; проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации; проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; поводить восстановление процесса и параметров функцианирования программных и программно-аппаратных, в том числе криптографических средств защиты информации	порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; типовых программных и программно-аппаратных средств защиты информации в ИТКС.	испытание и конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;

Перечень общих компетенций, элементы которых формируются в рамках дисциплины

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

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

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

Перечень профессиональных компетенций, элементы которых формируются в рамках дисциплины:

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.

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

ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации в соответствии с предъявляемыми требованиями.

1.3. Использование часов вариативной части ОП*

Вариативная часть в объеме 15 часов использована на расширение основных видов деятельности, к которым должен быть готов выпускник, освоивший образовательную программу, согласно получаемой квалификации, указанной в пункте 1.12 настоящего ФГОС СПО и введение дополнительных образовательных результатов МДК, выявленных как квалификационные дефициты в результате соотнесения требований WSR по компетенции Информационные кабельные сети. Содержание рабочей программы профессионального модуля ориентировано на следующие минимальные требования к навыкам (умениям), указанным в техническом описании компетенции:

Дополнительные знания, умения	Номер и наименование темы	Количество часов	Обоснование включения в рабочую программу
Проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации российского производства; Проводить техническое обслуживание и ремонт программно-аппаратных (в том числе	**Тема 2.1.** Основы криптографических методов защиты информации	10	Углубленная подготовка, современные требования опережающего образования
	Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	5	
	Итого:	15 часов	

криптографических) средств защиты информации российского производства. Программные и программно-аппаратные средства защиты информации в ИТКС российского производства; Криптографические средства защиты информации конфиденциального характера, которые применяются в ИТКС на основе российских стандартов;		

1.4. Количество часов, отводимое на освоение профессионального модуля

Объем учебной нагрузки: 550 часов

Из них на освоение МДК – 358 часов

МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты - 218 часов;

МДК.02.02. Криптографическая защита информации - 140 часов

Во взаимодействии с преподавателем – 330 часов, в том числе консультации – 2 часов

Самостоятельная работа обучающегося – 22 часов;

На практики учебную и производственную - 180часов.

Промежуточная аттестация в форме – экзамена по МДК (комплексный) и ПМ – 18 часов.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом деятельности (ВД) **Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

В результате изучения профессионального модуля студент должен освоить основной вид деятельности **Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты** и соответствующие ему профессиональные компетенции, и общие компетенции:

Перечень общих и профессиональных компетенций, элементы которых формируются в рамках дисциплины:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.
ВД 2	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты
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.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации в соответствии с предъявляемыми требованиями.

.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Промежуточная аттестация	Самостоят. работа	Консультации	Объем профессионального модуля, час.				
						Обучение по МДК			Практики	
						Всего	Лабораторных и практических занятий	Курсовых работ (проектов)	Учебная	Производственная
ПК 2.1 - 2.3; ОК 01 – 04; ОК 09, ОК 10	Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	218	6	10	2	202	88	20		
ПК 2.1 - 2.3; ОК 01 – 04; ОК 09, ОК 10	Раздел 2. Криптографическая защита информации	140		12		128	38			
ПК 2.1 - 2.3; ОК 01 – 04; ОК 09, ОК 10	Учебная практика	36							36	
ПК 2.1 - 2.3; ОК 01 – 04; ОК 09, ОК 10	Производственная практика, часов	144								144
	Промежуточная аттестация	12	12							
	Всего:	**550**	**18**	**22**	**2**	**330**	**126**	**20**	**36**	**144**

3.2. Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
ПМ.02.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты		**550**
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**218**
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**218**
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание**	
	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows XP. Windows 7. Windows 8. 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. Аппаратно-программные модули доверенной загрузки (АПМДЗ). Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. АПМДЗ Криптон-Замок, настройка системным администратором. Изучение настроек системного администратора АПМДЗ. АПМДЗ Криптон-Замок, настройки пользователя АПМДЗ. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ. Сектор HDD. Область памяти. Файл, папка, каталог.	20
	Практические занятия	
	Изучение средств идентификации аутентификации операционных систем. Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных	4

	записей. Назначение прав пользователя	
	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	4
	Настройка изолированной среды	2
	АПМДЗ Криптон-Замок, инициализация системного администратора, инициализация пользователя, проверка целостности среды	4
	Аппаратные средства шифрования Криптон-4,-8, настройка, эксплуатация	4
	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	4
	Восстановление информации типовыми средствами. Программы восстановление информации	4
Тема 1.2. Технологии разграничения доступа	**Содержание**	
	Архитектура подсистемы защиты операционной системы Windows Server 2016. Особенности ОС Windows Server 2016. 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. Active Directory. Комплексная система организации управления доступом. Инсталляция. Настройка. Аудит безопасности операционной системы. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. Функции межсетевых экранов (МЭ). 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.	26

	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.	
	Практические занятия	
	Программы надежного удаления информации	2
	Архивирование информации	2
	Программные средства резервного копирования. Настройка RAID-массивов	4
	Инсайдерская информация. Программы сбора информации о ПК	4
	Настройка межсетевого экрана	4
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание**	
	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. Туннелирование. 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.	22
	Практические занятия	
	Основные действия с виртуальной машиной	2

	Работа с контрольными точками	2
	Использование внешних устройств	2
	Работа с локальным хранилищем сертификатов в ОС WINDOWS	2
	Установка и настройка ПО eToken PKI Client	2
	Настройка ПО eToken PKI Client с помощью групповых политик	2
	Развертывание TMS в среде Active Directory	2
	Настройка TMS в среде Active Directory	2
	Настройка политик TMS	2
	Настройка использования виртуального токена	2
	Использование токена на рабочем месте администратора	2
	Установка и настройка СКЗИ «КриптоПро CSP»	2
	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами КриптоПро CSP	4
	Применение Secret Disk 4	2
	Применение Secret Disk Server NG	2
	Изучение основных возможностей ПО VIPNet Client	2
	Изучение настроек ПО VIPNet Client	2
	Изучение возможностей ПО Деловая почта	4
Тема 1.4. Технологии	**Содержание**	

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.	32
	Практические занятия	
	Изучение средств обнаружения атак	4
	Изучение антивирусных продуктов	4
Тема 1.5. Методы управления средствами защиты	**Содержание**	
	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.	10
	Самостоятельная работа	
	1. Проблемы обеспечения безопасности операционных системWindowsXP. Windows 7. Windows8. Linux. QNX. 2.Технологии аутентификации. 3.Аутентификация, авторизация и администрирование действий пользователя. 4.Пароли. PIN-коды. Методы надежного составления паролей	10

	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя. Оформление практических работ, отчетов и подготовка к их защите.	
Консультации		**2**
Промежуточная аттестация		**6**
Тематика курсовых работ (проектов)		
1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей. 2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей. 3. Анализ методов и средств анализа защищенности беспроводных сетей. 4. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения. 5. Виброакустические средства современных систем обеспечения информационной безопасности. 6. Средства защиты от ПЭМИН, современное состояние, проблемы и решения. 7. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 8. Средства обеспечения информационной безопасности банков данных. 9. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса). 10. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации. 11. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 12. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 13. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 14. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 15. Инструментальные средства анализа рисков информационной безопасности. 16. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками. 17. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).		
Раздел 2.Криптографическая защита информации		**140**
МДК 02.02.Криптографическая защита информации		**140**
Тема 2.1. Основы	**Содержание**	

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.	30
	Практические занятия	
	Стеганографические методы скрытия информации	2
	Бинарная арифметика. Модульная арифметика	2
	Применение методов шифрования перестановкой	2
	Применение методов шифрования заменой	2
	Применение методов шифрования многоалфавитной замены	2
	Криптоанализ методов перестановки	2
	Криптоанализ методов замены	2
	Компьютерное шифрование	2
Тема 2.2. Современные стандарты шифрования	**Содержание**	
	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.	30

	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.	
	Практические занятия	
	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	2
	Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	2
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	**Содержание**	
	Целостность сообщения. Случайная модель Oracle. 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 (ЭЦП). 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/MIME. 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	30

	скорости шифрования. Проблемы теории асимметричных алгоритмов.	
	Практические занятия	
	Разработка хэш-функции Разработка схемы простого пароля	2
	Разработка схемы динамического пароля Сертификаты открытого ключа	2
	Настройка и администрирование токена Настройка сервисов Рутокен PINPad	2
	Настройка сервисов Рутокен ЭЦП	2
	Настройка сервисов Рутокен Bluetooth	2
	Настройка сервисов Рутокен S	2
	Разработка алгоритма PGP	2
	Изучение протоколов SSL, TLS, IPSec	2
	Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	2
	Самостоятельная работа	12
	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. 7. Шифрование. Кодирование. Стеганография. Сжатие. 8. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. 9. Традиционные шифры замены. Шифры многоалфавитной замены. Частотность символов. 10. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. 11. Компьютерное шифрование. 12. Стандарт шифрования данных DES. Структура DES. Безопасность DES. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015.	

	13. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. 14. Асимметричное шифрование. Криптографическая система Эль-Гамаля. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.	
Учебная практика **Виды работ** Выбор, подключение, настройка межсетевого экрана. Администрирование межсетевого экрана. Ознакомление, подключение, настройка системы резервного копирования Администрирование системы резервного копирования. Ознакомление, подключение, настройка системы антивирусной защиты. Администрирование системы антивирусной защиты. Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции Составление алгоритма хеш-функции Составление алгоритма шифра Подключение, установка драйверов, настройка программных средств шифрования Криптон. Администрирование программных средств шифрования Криптон. Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. Администрирование аппаратных средств шифрования Криптон.		**36**
Производственная практика **Виды работ** Участие в организации работ по защите персональных компьютеров на предприятии Участие в организации работ по защите локальных сетей на предприятии Участие в организации работ по защите работ в глобальной сети интернет на предприятии Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. Администрирование систем безопасности проводной защищенной локальной сети. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. Администрирование систем безопасности беспроводной защищенной локальной сети. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей. Подключение, установка драйверов, настройка программных средств абонентского шифрования		**144**

Администрирование внедренных средств Настройка средств электронной подписи Администрирование средств электронной подписи Администрирование средств PKI	
Консультации	**2**
Промежуточная аттестация – экзамен (комплексный) по МДК 02.01 и 02.02 и экзамен по ПМ	**12**
Самостоятельная работа	**22**
Во взаимодействии с преподавателем	**330**
Учебная и производственная практика	**180**
Объем учебной нагрузки	**550**

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения.

Лаборатория «Программных и программно-аппаратных средств защиты информации» оборудована для проведения занятий лекционного типа, практических занятий, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования, находящегося в кабинете:

- рабочее место преподавателя (стол, стул, персональный компьютер);
- учебная мебель (столы, стулья);
- персональные компьютеры не ниже Core i3;
- коммутатор;
- интерактивная доска;
- проектор;
- аппаратно-программные средства обеспечения разграничения и контроля доступа пользователей АПМДЗ "КРИПТОН-ЗАМОК/К" (М-526А) в комплекте со считывателем смарт карт и устройством для подключения iButton;
- аппаратный шифратор для РС-совместимых компьютеров «КРИПТОН-8/PCI» в комплекте со считывателем смарт карт и устройством для подключения iButton;
- многофункциональный поисковый прибор ST 031 "Пиранья";
- абонентское устройство защиты телефонных линий «Гранит-8»;
- устройство защиты аналогового ТА «МП-1А»;
- устройство защиты цифрового ТА «МП-1А в евророзетке»;
- СИСТЕМНЫЙ КОМПЛЕКТ ARBYTE SILEX M115Q G3/G4400/8GB/4*1TB/RAID;
- SATA/k+m/2GLAN/500W/minitower;
- ПАК ViPNet IDS100 2.x;
- ПАК ViPNet Coordinator HW50 A 4.x;
- Рутокен PINPad;
- РУТОКЕН ЭЦП 2.0 память 64 Кбайт;
- Рутокен ЭЦП Bluetooth;
- Рутокен S 128КБ;
- USB-токен JaCarta PKI;
- S-Terra.

Используемое программное обеспечение:

- контракт № 29ЭА44-2018 от 06.09.2018 (Лицензия на использование JaCarta Management System от 14.09.2018 серийный номер 96d93439-984b-49be-93e0-db5e33051556 бессрочная, Лицензия на использование Secret Disk Server NG для файлового сервера на 10 пользователей (одновременных подключений)(лицензия сервера - E8E3-5990-3795-131C, лицензия администратора 0AEA-7027-899B-36D1) бессрочная, Передача права на использование ПО ViPNet Client for Windows 4.x (КС2)и ПО ViPNet Administrator 4.x (КС2)рег. Номер № 025-00173 от 21.11.2018 – бессрочная., Лицензия на право использования СКЗИ "КриптоПро CSP" версии 4.0 от 30.08.2018 срок неограничен;
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Microsoft Windows 10 Professional (предустановленное ПО, Контракт № 64ЭА44-2018 от 09.01.2019 с ООО «Азон», бессрочная);
- 7-Zip (свободно распространяемое ПО);

- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

Учебно-методическая документация.

Библиотека, читальный зал, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Перечень основного оборудования, находящегося в кабинете:
- рабочее место педагога-библиотекаря (стол, стул, персональный компьютер);
- учебная мебель (столы, стулья);
- персональные компьютеры.

Используемое программное обеспечение:
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление до-ступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

Кабинет для самостоятельной работы (компьютерный класс), оснащенный компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Перечень основного оборудования, находящегося в кабинете:
- учебная мебель (столы, стулья);
- персональные компьютеры;
- принтеры.

Используемое программное обеспечение:
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);

- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление до-ступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

Учебная аудитория «Кабинет подготовки к итоговой аттестации и защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты»

Перечень основного оборудования, находящегося в аудитории:
- мультимедийный проектор;
- экран;
- учебная мебель (столы, стулья, доска);
- учебно-наглядные пособия;
- ноутбук.

Используемое программное обеспечение:
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
- Python (свободно распространяемое ПО);
- Visual Basic (свободно распространяемое ПО);
- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

4.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе.

4.2.1. Печатные издания

Основная литература

1. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования / Е.Б.Белов, В.Н.Пржегорлинский. - М.: Издательский центр «Академия», 2017. – 336 с.

2. Богомазова Г.Н. Обеспечение информационной безопасности компьютерных сетей: учеб. для студ. учреждений сред. проф. образования / Г.Н.Богомазова. - М.: Издательский центр «Академия», 2017. – 224 с.

3. Рудаков, А.В. Технология разработки программных продуктов[Текст]: учебник для студ. учреждений сред. проф. образования/ А.В. Рудаков. – 11-е изд., стер. – М.: Издательский центр «Академия»,2017. – 208с.

4. Котов, Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов. — Новосибирск : Новосибирский государственный технический университет, 2016. — 59 с. — ISBN 978-5-7782-2959-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91377.html

5. Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие / Ю. А. Котов. — Новосибирск : Новосибирский государственный технический университет, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91227.html

Дополнительная литература

1. Майстренко, А. В. Мультимедийные средства обработки информации : учебное пособие для СПО / А. В. Майстренко, Н. В. Майстренко. — Саратов : Профобразование, 2020. — 81 с. — ISBN 978-5-4488-0734-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/90169.html

2. Соловьев, Н. А. Цифровая обработка информации в задачах и примерах : учебное пособие для СПО / Н. А. Соловьев, Н. А. Тишина, Л. А. Юркевская. — Саратов : Профобразование, 2020. — 122 с. — ISBN 978-5-4488-0596-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/92201.html

4.3. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья

Обучение по образовательным программам среднего профессионального образования обучающихся с ограниченными возможностями здоровья осуществляется на основе образовательных программ среднего профессионального образования, адаптированных при необходимости для обучения данной категории обучающихся.

Образование обучающихся с ограниченными возможностями здоровья организовано совместно с другими обучающимися.

Обучение по образовательным программам среднего профессионального образования обучающихся с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

В колледже созданы специальные условия для получения среднего профессионального образования, без которых невозможно или затруднено освоение образовательных программ обучающимися с ограниченными возможностями здоровья:

- создание специальных социально-бытовых условий, обеспечивающих возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения колледжа, а также их пребывания в указанных помещениях (пандусы с входными группами, телескопические пандусы, перекатные пандусы, гусеничные мобильные подъемники, поручни) для лиц с нарушениями опорно-двигательного аппарата;

- использование в образовательном процессе специальных методов обучения и воспитания (организация отдельного учебного места вблизи размещения

демонстрационного оборудования, дублирование основного содержания учебно-методического обеспечения в адаптированных раздаточных материалах, обеспечение облегченной практической деятельности на учебных занятиях, предупреждение признаков переутомления с помощью динамических пауз, соблюдение рационального акустического режима и обеспечение надлежащими звуковыми средствами воспроизведения информации, замедленный темп индивидуального обучения, многократное повторение, опора на сохранные анализаторы, функции и системы организма, опора на положительные личностные качества);

- обеспечение преподавателем-предметником организации технической помощи обучающимся с ограниченными возможностями здоровья;

- дублирование справочной информации, расписания учебных занятий в адаптированной форме в зданиях колледжа на информационных мониторах и наличие адаптированного официального сайта колледжа по адресу http://ctmtuci.ru/.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
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.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Текущий контроль в форме: - защиты практических занятий; - контрольных работ по темам МДК; - тестирование по темам МДК Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практик.
ПК 2.2.Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования	Комплексный экзамен по модулю. Защита курсового проекта. Промежуточная аттестация

информационно-телекоммуникационных системах и сетях.	программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	в форме экзамена по ПМ.
ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации в соответствии с предъявляемыми требованиями.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения	

	профессиональных задач;	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

Критерии оценки

«5»	Студент дает четкий и правильный ответ, выявляющий понимание материала и характеризующий прочные знания, излагает материал в логической последовательности с использованием специальной терминологии, свободно и легко устанавливает связь между теоретическими знаниями и практическими умениями. Самостоятельно выполняет задания практической работы, не нуждается в помощи преподавателя
«4»	Студент дает правильный ответ в определенной логической последовательности, способен устанавливать связи между теоретическими знаниями и практическими умениями. Овладел программным материалом, но допускает некоторую неполноту ответа и незначительные ошибки. При выполнении самостоятельной практической работы преподаватель оказывает незначительную помощь в виде наводящих вопросов.
«3»	Студент дает неполный ответ, построенный несвязно, но выявляет общее

	понимание вопроса, материал знает нетвердо, требует постоянной помощи преподавателя, дополнительного разъяснения этапов выполнения практического задания, наводящих вопросов.
«2»	Студент не дает ответа или допускает в нем существенные ошибки, которые не может исправить даже с помощью преподавателя. При выполнении практической работы постоянно нуждается в помощи преподавателя.