Воронежский колледж робототехники и компьютерных технологий

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D72D329BBD7B20000000072C4B0002
Владелец: Лукина Виктория Борисовна
Действителен: с 09.04.2021 до 09.04.2022

УТВЕРЖДАЮ
Директор колледжа
_____ Лукина В.Б.
«_____» _____ 2019 г.

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 среднего профессионального образования **10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»**

Квалификация выпускника: **техник по защите информации**

Воронеж
2019

Рабочая программа составлена на основании требований:

— Федерального государственного образовательного стандарта среднего профессионального образования №1551, утвержденного приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г.;

— учебного плана Воронежского колледжа робототехники и компьютерных технологий по специальности 10.02.04 — "Обеспечение информационной безопасности телекоммуникационных систем", утвержденного Педагогическим советом от 16.12.2019 г. протокол №1

Индекс — 10.02.04 ИБ

Составитель: преподаватель _____С.С. Куликов

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.02. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ (В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ЗАЩИТЫ»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности организовывать ремонтные, монтажные и наладочные работы по промышленному оборудованию и соответствующие ему профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 1	**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.

1.1.2. Перечень общих компетенций

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, необхо-

	димой 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.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– определения необходимых средств криптографической защиты информации; – использования программно-аппаратных криптографических средств защиты информации; – установки, настройки специализированного оборудования криптографической защиты информации; – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; – шифрования информации.
уметь	– выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; – определять рациональные методы и средства защиты на объектах и оценивать их эффективность; – производить установку и настройку типовых программно-аппаратных средств защиты информации; – пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
знать	– типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; – основные протоколы идентификации и аутентификации в телекоммуникационных системах; – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения программно-аппаратных средств обеспечения информационной безопасности в теле-

	коммуникационных системах; – основные способы противодействия – несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы; – основные понятия криптографии и типовые криптографические методы защиты информации;

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: **604 часов.**
Из них на освоение МДК – **301 часов:**

МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты- **216 часов;**

МДК.02.02 Криптографическая защита информации - **160 часов;**
На практики учебную и производственную -**216 часов.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	**Объем профессионального модуля, час.**					Самостоятельная работа1
			Обучение по МДК			Практики		
			всего, часов	Лабораторных и практических занятий	Курсовых работ (проектов)*	Учебная	Производственная (если предусмотрена рассредоточенная практика)	
ПК 2.1-2.3 ОК1-4, ОК9,10	Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	216	196	82	20			20
ПК 2.1-2.3 ОК1-4, ОК9,10	Раздел 2. Криптографическая защита информации	160	105	34	20			55
	Учебная практика	72				72		
ПК 2.1-2.3	Производственная	144					144	

Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

ОК1-4, ОК9,10	практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)							
	Промежуточная аттестация	12						
	Всего:	**604**	**301**	**116**	**40**	**72**	**144**	**75**

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (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		604
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		216
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		216
Тема 3.1. Обеспечение безопасности операционных систем	Содержание	19

	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.	
	Практические и лабораторные работы	**15**
	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав пользователя	3
	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	2
	Настройка изолированной среды	2
	АПМДЗ Криптон-замок инициализация системного администратора, инициализация	2

	пользователя, проверка целостности среды	
	Аппаратные средства шифрования Криптон 4,8 настройка, эксплуатация	2
	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	2
	Восстановление информации типовыми средствами Программы восстановление информации	2
Тема 3.2. Технологии разграничения доступа	**Содержание**	**19**
	Архитектура 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.	
	Практические и лабораторные работы	**13**
	Программы надежного удаления информации	2
	Архивирование информации	3
	Программные средства резервного копирования. Настройка RAID-массивов	3
	Инсайдерская информация. Программы сбора информации о ПК	2
	Настройка межсетевого экрана.	3
Тема 3.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание**	**18**
	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.	
	Практические и лабораторные работы	**50**
	Основные действия с виртуальной машиной	2
	Работа с контрольными точками	3
	Использование внешних устройств	3
	Работа с локальным хранилищем сертификатов в ОС WINDOWS	2
	Установка и настройка ПО eTokenPKIClient	3
	Настройка ПО eTokenPKIClient с помощью групповых политик	3
	Развертывание TMS в среде Active Directory	2
	Настройка TMS всреде Active Directory	3
	Настройка политик TMS	3
	Настройка использования виртуального токена	3
	Использование токена на рабочем месте администратора	3
	Установка и настройка СКЗИ «КриптоПроCSP»	3
	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	3
	Применение SecretDisk4	3
	Применение SecretDisk Server NG	3
	Изучение основных возможностей ПО VipNetClient	2
	Изучение настроек ПОVipNetClient	3

	Изучение возможностей ПО Деловая почта	3
Тема 3.4. Технологии обнаружения вторжений	**Содержание**	**19**
	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.	
	Практические и лабораторные работы	**4**
	Изучение средств обнаружения атак	2
	Изучение антивирусных продуктов	2
Тема 3.5. Методы	**Содержание**	**19**

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.	
Внеаудиторная (самостоятельная) учебная работа при изучении раздела ПМ		**20**
Рекомендуемая примерная тематика самостоятельной работы для разработчиков программ образовательной организации: 1.Комплексная система организации управления доступом. Инсталляция. Настройка. 2.Аудит безопасности операционной системы. 3.Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. 4.Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. 5.Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. 6.Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. 7.Концепция построения виртуальных защищенных сетей;. 8.Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура защищенного пакета. Варианты построения защищенных каналов. 9.Защита на канальном уровне. ПротоколыPPTP, L2F, L2TP. 10.Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. 11.Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. 12.Защита на прикладном уровне. ПротоколыPAP, CHAP,S/Key, SSO, Kerberos. 13.Функционирование системы управления средствами защиты. 14.Аудит безопасности информационной системы.		20

Учебная практика раздела МДК 02.01. **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.	
Производственная практика раздела 1 ПМ **Виды работ**	
Курсовой проект (работа) **Тематика курсовых проектов (работ):** 1. Проблемы обеспечения безопасности операционных систем Windows XP. Windows 7. Windows8. Linux. QNX. 2.Технологии аутентификации. 3.Аутентификация, авторизация и администрирование действий пользователя. 4.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.	**20**

8.Изучение настроек системного администратора АПМДЗ. 9.Сектор НЖМД. Область памяти. Файл, папка, каталог. 10.Разграничение доступа к объектам операционной системы.		
Раздел 2.Криптографическая защита информации		**160**
МДК 02.02.Криптографическая защита информации		**160**
Тема 2.1. Основы криптографических методов защиты информации	**Содержание**	
	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.	
	Практические и лабораторные работы	**8**

	Стеганографические методы скрытия информации	1
	Бинарная арифметика. Модульная арифметика	1
	Применение методов шифрования перестановкой	1
	Применение методов шифрования заменой	1
	Применение методов шифрования многоалфавитной замены	1
	Криптоанализ методов перестановки	1
	Криптоанализ методов замены	1
	Компьютерное шифрование	1
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. 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 и лабораторные работы	**4**

	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 Orac1e. 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. А3. А8.А5/3. 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.	
	Практические и лабораторные работы	**22**
	Разработка хэш-функции	1
	Разработка схемы простого пароля	1
	Разработка схемы динамического пароля	2
	Сертификаты открытого ключа	2
	Настройка и администрирование токена	2
	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 учебная работа при изучении раздела ПМ		
Рекомендуемая тематика внеаудиторной (самостоятельной0 работы: 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 раздела МДК02.02. **Виды работ** Проведение инструктажа по технике безопасности. 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.	
Производственная практика раздела 2 ПМ **Виды работ**	
Курсовой проект (работа) **Тематика курсовых проектов (работ):** 1. Модель угроз НСД на предприятии	**20**

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.	
Рекомендуемая тематика внеаудиторной самостоятельной работы: 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 информации в ИТКС.	**55**

Производственная практика (для программ подготовки специалистов среднего звена – (по профилю специальности)итоговая по модулю (если предусмотрена итоговая (концентрированная) 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 Администрирование внедренных средств Настройка средств электронной подписи Администрирование средств электронной подписи Администрирование средств PKI	**144**
Промежуточная аттестация	**12**
Всего по ПМ	**604**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы профессионального модуля требует наличия учебных кабинетов, лабораторий:

Лаборатория «Программных и программно-аппаратных средств защиты информации».

Лаборатория должна быть оснащена антивирусными программными комплексами; аппаратными средствами аутентификации пользователя; программно-аппаратными средствами управления доступом к данным и защиты (шифрования) информации; средствами защиты информации от НСД, блокирования доступа и нарушения целостности; программными средствами криптографической защиты информации; программными средствами выявления уязвимостей и оценки защищенности ИТКС, анализа сетевого трафика;

системы разграничения доступа;

межсетевые экраны;

средство криптографической защиты информации, реализующее функции удостоверяющего центра и создания виртуальных сетей;

комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Печатные издания

1. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябовд.Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2016. – 363 с.

2.Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов, 5-е изд. – Спб.: Питер, 2015. – 944 с. http://www.iprbookshop.ru/73702.html

3.Томаси У. Электронные системы связи.- М.: Техносфера, 2016. - 1360с. http://www.iprbookshop.ru/58897.html

4.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение

информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.

5.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013. – 172 с.

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

7.В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

8.Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012 http://www.iprbookshop.ru/87992.html

9.Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2009. - 192с.

10.Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с. http://www.iprbookshop.ru/66445.html

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

http://www.morion.ru/

http://www.nateks.ru/

http://www.iskratel.com/

http://www.ps-ufa.ru/

http://3m.com/

http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»

3.2.3. Дополнительные источники

Дополнительные источники:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
- Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в инфор-

мационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
  от 30 августа 2002 г. № 282.
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
  от 31 августа 2010 г. № 416/489.
- Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
- Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
- Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
- ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели

менеджмента безопасности информационных и телекоммуникационных технологий

- ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
- ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
- ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
- ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
- ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
- ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
- ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
- ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
- ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ро-

стехрегулирование, 2006.
- ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
  Номенклатура показателей качества. Ростехрегулирование, 2005.
- ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
- ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
- ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
- ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
- Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Отечественные журналы:

"InformationSecurity/ Информационная безопасность"
Системный администратор
Компьютер ПРЕСС
Системы безопасности. Журнал для руководителей и специалистов в области
безопасности
Сети и системы связи
Защита информации. Инсайд: Информационно-методический журнал
Информационная безопасность регионов: Научно-практический журнал

Интернет Ресурсы
http://cryptogrof.ru/

4. 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. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности 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 установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение

ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС и их диагностику, обнаружение отказов, формировать предложения по их устранению	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования 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;	Экспертное наблюдение
ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности 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 конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение

ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей	- 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;	Экспертное наблюдение
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;	Экспертное наблюдение Экзамен
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;	Экспертное наблюдение Экзамен

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
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);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен

ПРИЛОЖЕНИЕ 1

Воронежский колледж робототехники и компьютерных технологий

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D72D329BBD7B20000000072C4B0002
Владелец: Лукина Виктория Борисовна
Действителен: с 09.04.2021 до 09.04.2022

УТВЕРЖДАЮ

Директор колледжа

_____ Лукина В.Б.

«_____» _____ 2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

дисциплины

«ПМ.02. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ (В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ЗАЩИТЫ»

для специальности среднего профессионального образования **10.02.04" Обеспечение информационной безопасности телекоммуникационных систем "**

Квалификация выпускника: **техник по защите информации**.

Воронеж
2019

Цель фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты». Перечень видов оценочных средств соответствует Рабочей программе дисциплины.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля в форме индивидуальных заданий при выполнении цикла лабораторных работ и промежуточной аттестации в форме вопросов и заданий (могут быть заданы как в форме билета, так и экзаменационного теста) к экзамену.

Структура и содержание заданий - задания разработаны в соответствии с рабочей программой дисциплины «защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты».

1. Паспорт фонда оценочных средств

Результатом освоения учебной дисциплины являются предусмотренные ФГОС по специальности умения и знания, направленные на формирование общих и профессиональных компетенций.

Таблица 1

№ п/п	Код компетенции	Содержание компетенции	Планируемые результаты обучения	Наименование оценочного средства
1	ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (са- **Знания:** актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы
2	ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска **Знания:** номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации	**Задание** на выполнение индивидуального варианта лабораторной работы
3	ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования **Знания:** содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования	**Задание** на выполнение индивидуального варианта лабораторной работы

4	ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности **Знания:** психология коллектива; психология личности; основы проектной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы
5	ОК 09	Использовать информационные технологии в профессиональной деятельности.	**Умения:** применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение **Знания:** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы
6	ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы **Знания:** правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности	**Задание** на выполнение индивидуального варианта лабораторной работы
7	ВД 1	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты .	**Знания**: типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; основные протоколы идентификации и аутентификации в телекоммуникационных системах; состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-	**Задание** на выполнение индивидуального варианта лабораторной работы

			телекоммуникационной системы; основные понятия криптографии и типовые криптографические методы защиты информации; **Умения**: выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; определять рациональные методы и средства защиты на объектах и оценивать их эффективность; производить установку и настройку типовых программно-аппаратных средств защиты информации; пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;.	
8	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	**Умения**: 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; **Знания**: способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; типовых программных и программно-аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;	**Задание** на выполнение индивидуального варианта лабораторной работы
9	ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	**Умения**: выявлять и оценивать угрозы безопасности информации в ИТКС; проводить контроль показателей и процесса функционирования 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;	**Задание** на выполнение индивидуального варианта лабораторной работы

			Знания: возможных угроз безопасности информации в ИТКС; способов защиты информации от НСД и специальных воздействий на нее; порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; 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;	
10	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 предъявленными требованиями	**Умения**: 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; **Знания**: возможных угроз безопасности информации в ИТКС; способов защиты информации НСД и специальных воздействий на нее; типовых программных и программно-аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации.	**Задание** на выполнение индивидуального варианта лабораторной работы

Формой промежуточной аттестации по учебной дисциплине является

экзамен

указать форму аттестации, предусмотренную учебным планом

2. Формы контроля и оценивания элементов учебной дисциплины

В результате текущей аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих и профессиональных компетенций.

Таблица 2

Раздел / тема дисциплины	**Проверяемые У, З, ОК, ПК**	**Форма текущего контроля и оценивания**
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	ПК 2.1-2.3 ОК1-4, ОК 09,10	Самостоятельная работа
Тема 1.1. Обеспечение безопасности операционных систем	ПК 2.1-2.3 ОК1-4, ОК 09,10	Практическое занятие №№ 1-7
Тема 1.2. Технологии разграничения доступа	ПК 2.1-2.3 ОК1-4, ОК 09,10	Практическое занятие №№ 8-13
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	ПК 2.1-2.3 ОК1-4, ОК 09,10	Практическое занятие №№ 14-32
Тема 1.4. Технологии обнаружения вторжений	ПК 2.1-2.3 ОК1-4, ОК 09,10	Практическое занятие №№ 33-34

Тема 1.5. Методы управления средствами защиты	ПК 2.1-2.3 ОК1-4, ОК 09,10	Самостоятельная работа
Раздел 2. Криптографическая защита информации	ПК 2.1-2.3 ОК1-4, ОК 09,10	Самостоятельная работа
Тема 2.1. Основы криптографических методов защиты информации	ПК 2.1-2.3 ОК1-4, ОК 09,10	Практическое занятие №№ 1-8
Тема 2.2. Современные стандарты шифрования	ПК 2.1-2.3 ОК1-4, ОК 09,10	Практическое занятие №№ 9-10
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	ПК 2.1-2.3 ОК1-4, ОК 09,10	Практическое занятие №№ 11-22

3. Оценка освоения учебной дисциплины

3.1 Тематика курсовых работ

1. Проблемы обеспечения безопасности операционных систем Windows XP. Windows 7. Windows8. Linux. QNX.
2.Технологии аутентификации.
3.Аутентификация, авторизация и администрирование действий пользователя.
4.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.
9.Сектор НЖМД. Область памяти. Файл, папка, каталог.
10.Разграничение доступа к объектам операционной системы.
11. Модель угроз НСД на предприятии
12. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии
13. Проведение классификации ПО по требованиям ФСТЭК на предприятии
14. Проведение классификации МЭ по требованиям ФСТЭК на предприятии
15. Построение модели нарушителя по требованиям ФСТЭК на предприятии
16. Построение модели нарушителя по требованиям ФСБ на предприятии
17. Модель угроз безопасности ИС персональных данных на предприятии
18. Комплексная модель защиты информации на предприятии.
19. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
20. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
21. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
22. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
23. Проблема защиты информации в облачных хранилищах данных и ЦОДах
24. Защита сред виртуализации.

4. Контрольно-оценочные материалы для промежуточной аттестации по учебной дисциплине

Оценка освоения дисциплины предусматривает проведение экзамена

указать форму аттестации, предусмотренную учебным планом

4.1. Вопросы (задания) к экзамену по дисциплине:

1. Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows XP. Windows 7. Windows8. Linux. QNX и другие операционные системы.
2. Технологии аутентификации.
3. Аутентификация, авторизация и администрирование действий пользователя
4. Методы аутентификации
5. Пароли. PIN-коды. Методы надежного составления паролей.
6. Строгая аутентификация
7. Односторонняя аутентификация. Двухсторонняя аутентификация
8. Аппаратно-программные средства идентификации и аутентификации.
9. Токены. Смарт-карты. Виртуальные ключи.
10. Программно-аппаратные модули доверенной загрузки.
11. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ.
12. АПМДЗ Криптон –Замок системный администратор.
13. Изучение настроек системного администратора АПМДЗ.
14. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ.
15. Ограничения действий пользователя. Идентификация. Журнал регистрации событий.
16. Настройки целостности среды АПМДЗ
17. Сектор НЖМД. Область памяти. Файл, папка, каталог.
18. Архитектура подсистемы защиты операционной системы Windows Server2016.
19. Особенности ОС Windows Server2016. Возможности администратора.
20. Разграничение доступа к объектам операционной системы.
21. Модели доступа. Дискреционная модель. Мандатная модель. Роли.
22. Локальная политика безопасности.
23. Настройка локальной политики безопасности. Администрирование системы.
24. Изолированная программная среда.
25. Способы организации. Методы применения.
26. ActiveDirectory.

5. Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Индикаторы компетенции	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**отлично**
Полнота знаний	Уровень знаний ниже минимальных требований. Лабораторные работы выполнены не в полном объеме	Минимально допустимый уровень знаний. Лабораторные работы выполнены в полном объеме	Уровень знаний в объеме, соответствующем программе подготовки. Лабораторные работы выполнены в полном объеме	Уровень знаний в объеме, соответствующем программе подготовки, лабораторные работы выполнены в полном объеме
Наличие умений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи. Индивидуальные задачи решены по типовому шаблону.	Продемонстрированы все основные умения. Решены типовые задачи. Выполнены индивидуальные задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи, выполнены все индивидуальные задания в полном объеме.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач.	Сформированность компетенции в целом соответствует требованиям, но есть недочеты. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по некоторым профессиональным задачам.	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий	Ниже среднего	Средний	Высокий