ДЕПАРТАМЕНТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ТОМСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТОМСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»

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

Томск
2020 год

ОДОБРЕНО
Предметной (цикловой) комиссией
информационных технологий
Председатель
_____А.М. Вернигора
Протокол № 8
от «15 » июня 2020 г.

УТВЕРЖДАЮ
Зам. директора по УМР
_____ Л.В. Сидакова
от «29 » июня 2020 г.

Заведующий библиотекой
_____О.А Пинаева
от «22 » июня 2020 г.

Рабочая программа учебной дисциплины разработана на основе приказа Министерства образования и науки Российской Федерации от 09.12.2016 № 1551 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования» по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Организация-разработчик: ОГБПОУ «Томский индустриальный техникум»

Разработчик:

Терехова Валентина Андреевна, преподаватель первой квалификационной категории

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

1.2. Цель и планируемые результаты освоения профессионального модуля

Профессиональный модуль направлен на формирование у студента базовых представлений об основных видах профессиональной деятельности и приобретение необходимых профессиональных компетенций:

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности: эксплуатация информационно-телекоммуникационных систем и сетей и соответствующие ему профессиональные и общие компетенции:

1.2.1. Перечень общих компетенций

Код	Наименование общих 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.

1.2.2. Перечень профессиональных компетенций

Выпускник, освоивший программу СПО по профессии (специальности) должен обладать профессиональными компетенциями

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.

1.2.3. В результате освоения профессионального модуля будут освоены следующие действия, умения и знания:

Спецификация ПК/ разделов профессионального модуля

Коды формируемых компетенций	**Действия (дескрипторы)**	**Умения**	**Знания**
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных 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.	установка, настройка, испытание и конфигурирование программных и программно-аппаратных средств защиты от несанкционированного доступа;	выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;	состава и возможности типовых конфигураций программно-аппаратных средств защиты информации;
	использовать программно-аппаратные криптографические средства защиты информации;	определять рациональные методы и средства защиты на объектах и оценивать их эффективность;	основных способов противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;

ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	поддержание бесперебойной работы программных и программно-аппаратных средств защиты информации;	производить установку и настройку типовых программно-аппаратных средств защиты информации;	особенностей применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;
	установка, настройка специализированного оборудования криптографической защиты информации;		
	применение программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;		
Раздел 2. Криптографическая защита информации			
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.	использование методов шифрования информации.	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации.	основных протоколов идентификации и аутентификации в телекоммуникационных системах
			типовых криптографических алгоритмов, применяемых в защищенных телекоммуникационных системах;
			Основных понятий криптографии и типовых криптографических методов защиты информации.

1.3. Количество часов, отводимое на освоение профессионального модуля

Всего часов максимальной учебной нагрузки: **536 часов.**

Из них на освоение МДК**:**

МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты - **220 часов;**

МДК.02.02 Криптографическая защита информации - **136 часов;**

На практики учебную и производственную - **180 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 работа
			Обучение по МДК			Практики		
			всего, часов	Лабораторных и практических занятий	Курсовых работ (проектов)	Учебная	Производственная	
ПК 2.2-2.3 ОК 01-03	Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	220	204	84	20			16
ПК 2.3 ОК 01-03	Раздел 2. Криптографическая защита информации	136	136	78	10			
	Учебная практика	36						
ПК 2.1-2.3 ОК 1-4, ОК 9,10	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	144						
	Всего:	536	340	162	30			16

2.2. Тематический план и содержание профессионального модуля (ПМ.02)

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
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			**220**
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			220
Тема 1.1. Обеспечение безопасности операционных систем	Содержание	Уровень освоения	
		2,3	

	1. Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows XP. Windows 7. Windows 8. 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. Настройки целостности среды АПМДЗ 16. Сектор НЖМД. Область памяти. Файл, папка, каталог		20
	Тематика практических занятий		***22***
	1. Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя		2
	2. Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита		2
	3. Настройка изолированной среды		2
	4. АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды		4
	5. Аппаратные средства шифрования Криптон 4,8 настройка, эксплуатация		4
	6. Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование		4
	7. Восстановление информации типовыми средствами Программы восстановление информации		4
	Консультации		2
Тема 1.2. Технологии разграничения доступа	Содержание	Уровень освоения	

	1. Архитектура подсистемы защиты операционной системы Windows Server 2016. 2. Особенности ОС Windows Server 2016. Возможности администратора. 3. Разграничение доступа к объектам операционной системы. 4. Модели доступа. Дискреционная модель. Мандатная модель. Роли. 5. Локальная политика безопасности. 6. Настройка локальной политики безопасности. Администрирование системы. 7. Изолированная программная среда. 8. Способы организации. Методы применения. ActiveDirectory. 9. Комплексная система организации управления доступом. Инсталяция. Настройка. 10. Аудит безопасности операционной системы. 11. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. 12. Функции межсетевых экранов. 13. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. 14. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. 15. Особенности функционирования межсетевых экранов. 16. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. 17. Схемы защиты на базе межсетевых экранов. 18. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. 19. Тестирование межсетевых экранов. 20. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.	2,3	26
	Тематика практических занятий		***14***
	1. Программы надежного удаления информации		4
	2. Архивирование информации		2
	3. Программные средства резервного копирования. Настройка RAID-массивов		2
	4. Инсайдерская информация. Программы сбора информации о ПК		4
	5. Настройка межсетевого экрана.		2
	Консультации		2

Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Содержание	Уровень освоения	
	1. Проблемы информационной безопасности сетей. 2. 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. 3. Концепция построения виртуальных защищенных сетей. 4. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. 5. VPN – решения для построения защищенных сетей. 6. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. 7. Защита на канальном уровне. 8. Протоколы PPTP, L2F, L2TP. 9. Протоколы формирования защищенных каналов на сеансовом уровне. 10. Протоколы SSL, TLS, SOCKS. 11. Защита на сетевом уровне. 12. Архитектура средств безопасности IPSec, AH, ESP. 13. Защита на прикладном уровне. 14. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	2,3	18
	Тематика практических занятий		***40***
	1. Основные действия с виртуальной машиной		2
	2. Работа с контрольными точками		2
	3. Использование внешних устройств		2
	4. Работа с локальным хранилищем сертификатов в ОС WINDOWS		2
	5. Установка и настройка ПО eTokenPKIClient		2
	6. Настройка ПО eTokenPKIClient с помощью групповых политик		2
	7. Развертывание TMS в среде Active Directory		2
	8. Настройка TMS в среде Active Directory		4
	9. Настройка политик TMS		2
	10. Настройка использования виртуального токена		2

	11. Использование токена на рабочем месте администратора		2
	12. Установка и настройка СКЗИ «КриптоПроCSP»		2
	13. Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP		4
	14. Применение SecretDisk4		2
	15. Применение SecretDisk Server NG		2
	16. Изучение основных возможностей ПО VipNetClient		2
	17. Изучение настроекПОVipNetClient		2
	18. Изучение возможностей ПО Деловая почта		2
	Консультации		2
Тема 1.4. Технологии обнаружения вторжений	Содержание	Уровень освоения	14
	1. Технология обнаружения атак. 2. Концепция адаптивного управления безопасностью. Технология анализа защищенности. 3. Средства анализа защищенности сетевых протоколов и сервисов. 4. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. 5. Средства обнаружения сетевых атак. 6. 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. 7. Обзор современных средств обнаружения атак. 8. Технологии защиты от вирусов. 9. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.		
	Тематика практических занятий		***8***
	1. Изучение средств обнаружения атак		4
	2. Изучение антивирусных продуктов		4
	Консультации		2

Тема 1.5. Методы управления средствами защиты	Содержание	Уровень освоения	
	1. Методы управления средствами сетевой защиты. 2. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. 3. Аудит безопасности информационной системы. 4. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. 5. Обзор современных систем управления сетевой защитой. 6. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.	3	12
	Консультации		2
Внеаудиторная (самостоятельная) учебная работа при изучении раздела ПМ			**16**
Рекомендуемая примерная тематика самостоятельной работы для разработчиков программ образовательной организации: 1. Проблемы обеспечения безопасности операционных системWindows XP. Windows 7. Windows 8. 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. Комплексная система организации управления доступом. Инсталяция. Настройка. 12. Аудит безопасности операционной системы. 13. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. 14. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. 15. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. 16. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. 17. Концепция построения виртуальных защищенных сетей;. 18. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура защищенного пакета. Варианты построения защищенных каналов. 19.Защита на канальном уровне. ПротоколыPPTP, L2F, L2TP. 20.Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS.		

21.Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. 22.Защита на прикладном уровне. ПротоколыPAP, CHAP,S/Key, SSO, Kerberos. 23.Функционирование системы управления средствами защиты. 24.Аудит безопасности информационной системы.	
Курсовой проект (работа) Тематика курсовых проектов (работ): 1. Модель угроз НСД на предприятии 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии 6. Построение модели нарушителя по требованиям ФСБ на предприятии 7. Модель угроз безопасности ИС персональных данных на предприятии 8. Комплексная модель защиты информации на предприятии. 9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 13. Проблема защиты информации в облачных хранилищах данных и ЦОДах 14. Защита сред виртуализации.	20
Всего	220

Раздел 2. Криптографическая защита информации		**136**
МДК 02.02.Криптографическая защита информации		136
Тема 2.1. Основы криптографических методов защиты информации	Содержание 1. Свойства информационной безопасности. 2. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности. 3. Криптографические методы. 4. Шифрование. Кодирование. Стеганография. Сжатие. 5. Математика криптографии. 6. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. 7. Традиционные шифры перестановки. 8. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. 9. Традиционные шифры замены. 10. Шифры замены. Шифры многоалфавитной замены. Частотность символов. 11. Криптоанализ. 12. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. 13. Компьютерное шифрование. 14. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	12
	Тематика практических занятий	***32***
	1. Стеганографические методы скрытия информации	4
	2. Бинарная арифметика. Модульная арифметика	4
	3. Применение методов шифрования перестановкой	4
	4. Применение методов шифрования заменой	4
	5. Применение методов шифрования многоалфавитной замены	4
	6. Криптоанализ методов перестановки	4
	7. Криптоанализ методов замены	4
	Компьютерное шифрование	4
	Консультации	2

Тема 2.2. Современные стандарты шифрования	Содержание	
	1. Симметричное шифрование. 2. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES. 3. Усовершенствованный стандарт шифрования AES. 4. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES. 5. Российские стандарты симметричного шифрования . 6. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. 7. Проблема распределения ключей симметричного шифрования. 8. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. 9. Асимметричное шифрование. 10. 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. 11. Российские стандарты асимметричного шифрования. 12. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.	16
	Тематика практических занятий	***4***
	1. Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	2
	2.Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители сообщения.	2
	Консультации	2
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	Содержание	
	1. Случайная модель Огас1е. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции. 2. Электронная цифровая подпись. 3. 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. 4. Установление подлинности объекта. 5. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. 6. Проблемы распределения открытого ключа асимметричного шифрования. 7. Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI.	14

	8. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. 9. Электронная почта. Архитектура e-mail. PGP. S/M1ME . 10. Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. 11. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети 12. Защита информации в сетях организованных по технологии беспроводного доступа. 13. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16. 14. Защита информации в сетях сотовой связи. 15. A3. A8.A5/3. Атаки на алгоритмы. 16. Перспективы развития беспроводной мобильной связи. 17. Криптовалюты. 18. Биткоин. Блокчейн-системы Ethereum. 19. Перспективы развития криптографии. 20. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.	
	Тематика практических занятий	***42***
	1. Разработка хэш-функции	4
	2. Разработка схемы простого пароля	4
	3. Разработка схемы динамического пароля	4
	4. Сертификаты открытого ключа	4
	5. Настройка и администрирование токена	4
	6. Настройка сервисов Рутокен-PinPad	4
	7. Настройка сервисов Рутокен-ЭЦП	4
	8. Настройка сервисов Рутокен–Bluetooth	4
	9. Настройка сервисов Рутокен–S	4
	10. Разработка алгоритма PGP	2
	11. Изучение протоколов SSL, TLS, IPSec	2
	12. Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	2
	Консультации	2

Учебная практика раздела МДК 02.02. Виды работ: 1. Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции 2. Составление алгоритма шифра 3. Подключение, установка драйверов, настройка программных средств шифрования Криптон. 4. Администрирование программных средств шифрования Криптон 5. Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. *6.* Администрирование аппаратных средств шифрования Криптон.	36
Курсовой проект (работа) Тематика курсовых проектов (работ): 1. Модель угроз НСД на предприятии 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии 6. Построение модели нарушителя по требованиям ФСБ на предприятии 7. Модель угроз безопасности ИС персональных данных на предприятии 8. Комплексная модель защиты информации на предприятии. 9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 13. Проблема защиты информации в облачных хранилищах данных и ЦОДах 14. Защита сред виртуализации.	10
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.	

Производственная практика (для программ подготовки специалистов среднего звена – (по профилю специальности) итоговая по модулю (если предусмотрена итоговая (концентрированная) практика) Виды работ: 1. Участие в организации работ по защите персональных компьютеров на предприятии 2. Участие в организации работ по защите локальных сетей на предприятии 3. Участие в организации работ по защите работ в глобальной сети интернет на предприятии 4. Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. 5. Администрирование систем безопасности проводной защищенной локальной сети. 6. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. 7. Администрирование систем безопасности беспроводной защищенной локальной сети. 8. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. 9. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей 10. Подключение, установка драйверов, настройка программных средств абонентского шифрования 11. Администрирование внедренных средств 12. Настройка средств электронной подписи 13. Администрирование средств электронной подписи 14. Администрирование средств PKI	144
Всего по ПМ 02	**536**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Реализации программы профессионального модуля предполагает наличия:

для МДК.02.01, МДК.02.02, УП.02:

- учебной аудитории № 405 «Лаборатория информационно-телекоммуникационных систем и сетей»

- Оборудование: Презентационное оборудование, интерактивная панель, 12 ПК, учебная мебель.

- Учебно-наглядное пособие: комплект УМК по дисциплине (дидактические материалы, контрольно-оценочные средства, наглядные материалы и т.д.)

- Программное обеспечение: ОС Linux Debian 10

3.2. Информационное обеспечение обучения

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

МДК.02.01

Основная литература:

Юрайт (Казарин), Знаниум (Братко)

МДК.02.02

Дополнительная литература

Рябко Б.Я. , Фионов А.Н. Криптография в информационном мире./ Б.Я.Рябко, А.Н.Фионов. – М.: Горячая линия – Телеком, 2018. – 300с.: ил. – ISBN 978-5-9912-09729-4. - Текст: непосредственный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Преподаватели обеспечивают организацию и проведение текущего, промежуточного и итогового контроля. Текущий контроль проводиться преподавателем в процессе проведения практических работ, тестирования, устных и письменных опросов, а так же выполнения индивидуальных заданий – рефератов, домашних работ.

Обучение по междисциплинарным курсам завершается промежуточной аттестацией в форме экзамена.

Ожидаемый результат	**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; - проводить конфигурирование 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; - проводить техническое обслуживание и ремонт 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