Министерство образования и молодежной политики Свердловской области
Государственное автономное профессиональное образовательное учреждение
Свердловской области
«Уральский радиотехнический колледж им. А.С. Попова»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 06ADA45E000EAEACA648DBB10A49EF8273
Владелец: Бурганов Николай Тафкильевич
Действителен: с 30.12.2021 до 30.03.2023

УТВЕРЖДАЮ:
Зам. Директора по УМР
_____/ С.Н. Меньшикова /
«___ » _____2022 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

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Екатеринбург
2022

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 4

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 8

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 27

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 31

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ 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:

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. Общие компетенции:

Код	**Наименование видов деятельности и профессиональных компетенций**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

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

1.4. Количество часов, отводимое на освоение профессионального модуля

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	**643**
В том числе вариативная часть, направленная на усиление обязательной части программы профессионального модуля	172
из них на освоение МДК.01.01	274
из них на освоение МДК.01.02	177
Обязательная аудиторная учебная нагрузка (всего)	595
в том числе:	
теоретическое обучение	273
практические занятия	112
лабораторные работы	
курсовое проектирование	30
Самостоятельная работа обучающегося (всего)	20
Учебная практика	110
Производственная практика	74
Консультации	12
Промежуточная аттестация, в том числе: Итоговая аттестация в форме Квалификационного Экзамена по модулю	16

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура и содержание профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Занятия во взаимодействии с преподавателем, час				Самостоятельная работа	Консультации
			Лекций	Лабораторных и практических занятий	Курсовых работ (проектов)	Промежуточная аттестация		
ПК 2.1-ПК 2.3 ОК 01-04 ОК 09-10	МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	274	188	68	-	4	10	4
	МДК.02.02.Криптографическая защита информации	177	85	44	30	4	10	4
ПК 2.1-ПК 2.3 ОК 01-04 ОК 09-10	УП.02.01 Учебная практика	110	108					2
	ПП.02.01 Производственная практика	74	72					2
ПМ.02.ЭК Квалификационный экзамен		8	-			8	-	
	Всего:	**643**						

2.2. Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая 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		
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**274**
Тема 3.1. Обеспечение безопасности операционных систем	**Содержание**	**76**
	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows XP. Windows 7. Windows8. Linux. QNX и другие операционные системы.	4
	Технологии аутентификации.	4
	Аутентификация, авторизация и администрирование действий пользователя.	2
	Методы аутентификации	4
	Пароли. PIN-коды. Методы надежного составления паролей.	2
	Строгая аутентификация.	4
	Односторонняя аутентификация. Двухсторонняя аутентификация	4
	Аппаратно-программные средства идентификации и аутентификации.	2
	Токены. Смарт-карты. Виртуальные ключи.	4
	Программно-аппаратные модули доверенной загрузки.	4
	Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ.	4
	АПМДЗ Криптон –Замок системный администратор.	4
	Изучение настроек системного администратора АПМДЗ.	4
	АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ.	4
	Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ	4
	Сектор НЖМД. Область памяти. Файл, папка, каталог.	4
	Практические и лабораторные работы	**18**
	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя	
	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	
	Настройка изолированной среды	

	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	
	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация	
	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	
	Восстановление информации типовыми средствами Программы восстановление информации	
Тема3.2. Технологии разграничения доступа	**Содержание**	**82**
	Архитектура подсистемы защиты операционной системы Windows Server2016.	4
	Особенности ОС Windows Server2016. Возможности администратора.	4
	Разграничение доступа к объектам операционной системы.	4
	Модели доступа. Дискреционная модель. Мандатная модель. Роли.	4
	Локальная политика безопасности.	4
	Настройка локальной политики безопасности. Администрирование системы.	4
	Изолированная программная среда.	4
	Способы организации. Методы применения.	4
	ActiveDirectory.	2
	Комплексная система организации управления доступом. Инсталяция. Настройка.	4
	Аудит безопасности операционной системы.	2
	Методы проведения контрольных проверочных мероприятий. Программные средства аудита.	4
	Функции межсетевых экранов.	4
	Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика.	2
	Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.	4
	Особенности функционирования межсетевых экранов.	2
	Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня.	4
	Схемы защиты на базе межсетевых экранов.	2
	Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ.	4
	Тестирование межсетевых экранов.	4
	Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.	2
	Практические и лабораторные работы	**10**
	Программы надежного удаления информации	
	Архивирование информации	
	Программные средства резервного копирования. Настройка RAID-массивов	
	Инсайдерская информация. Программы сбора информации о ПК	
	Настройка межсетевого экрана.	
Тема 3.3. Обеспечение	**Содержание**	**64**

информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	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.	2
	Концепция построения виртуальных защищенных сетей.	2
	Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование.	2
	VPN – решения для построения защищенных сетей.	2
	Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация.	2
	Защита на канальном уровне.	2
	Протоколы PPTP, L2F, L2TP.	2
	Протоколы формирования защищенных каналов на сеансовом уровне.	2
	Протоколы SSL, TLS, SOCKS.	2
	Защита на сетевом уровне.	2
	Архитектура средств безопасности IPSec, AH, ESP.	2
	Защита на прикладном уровне.	2
	Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	2
	Практические и лабораторные работы	**36**
	Основные действия с виртуальной машиной	2
	Работа с контрольными точками	2
	Использование внешних устройств	2
	Работа с локальным хранилищем сертификатов в ОС WINDOWS	2
	Установка и настройка ПО eTokenPKIClient	2
	Настройка ПО eTokenPKIClient с помощью групповых политик	2
	Развертывание TMS в среде Active Directory	2
	Настройка TMS всреде Active Directory	2
	Настройкаполитик TMS	2
	Настройка использования виртуального токена	2
	Использование токена на рабочем месте администратора	2
	Установка и настройка СКЗИ «КриптоПроCSP»	2
	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	2
	Применение SecretDisk4	2
	Применение SecretDisk Server NG	2
	Изучение основных возможностей ПО VipNetClient	2

	Изучение настроекПОVipNetClient	2
	Изучение возможностей ПО Деловая почта	2
Тема 3.4. Технологии обнаружения вторжений	**Содержание**	**22**
	Технология обнаружения атак.	2
	Концепция адаптивного управления безопасностью. Технология анализа защищенности.	2
	Средства анализа защищенности сетевых протоколов и сервисов.	2
	Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.	2
	Средства обнаружения сетевых атак.	2
	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.	2
	Обзор современных средств обнаружения атак.	2
	Технологии защиты от вирусов.	2
	Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусовЖизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.	2
	Практические и лабораторные работы	**4**
	Изучение средств обнаружения атак	
	Изучение антивирусных продуктов	
Тема 3.5. Методы управления средствами защиты	**Содержание**	**12**
	Методы управления средствами сетевой защиты.	2
	Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты.	2
	Аудит безопасности информационной системы.	2
	Мониторинг безопасности системы. Программные средства проведения аудита безопасности.	2
	Обзор современных систем управления сетевой защитой.	2
	Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.	2
Самостоятельная учебная работа при изучении раздела ПМ:		**10**
1. Проблемы обеспечения безопасности операционных системWindowsXP. Windows 7. Windows8. Linux. QNX.		
2.Технологии аутентификации.		
3.Аутентификация, авторизация и администрирование действий пользователя.		
4.Пароли. PIN-коды. Методы надежного составления паролей.		
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. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.3.сыМЭ. Требования ФСТЭК к документации на оборудование ИТКС.		
23.Функционирование системы управления средствами защиты.		
24.Аудит безопасности информационной системы.		
Консультации		*4*
Промежуточная аттестация по МДК.02.01 в форме дифференцированного зачета		*4*
Раздел 2.Криптографическая защита информации		
МДК 02.02.Криптографическая защита информации		**177**
Тема 2.1. Основы криптографических методов защиты информации	**Содержание**	**41**
	Свойства информационной безопасности.	2
	Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности.	2
	Криптографические методы.	2
	Шифрование. Кодирование. Стеганография. Сжатие.	
	Математика криптографии.	2
	Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение.	2
	Традиционные шифры перестановки.	2
	Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования.	2
	Традиционные шифры замены.	1
	Шифры замены. Шифры многоалфавитной замены. Частотность символов.	2
	Криптоанализ.	2

	Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста .	2
	Компьютерное шифрование.	2
	Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	2
	Практические и лабораторные работы	**16**
	Стеганографические методы скрытия информации	2
	Бинарная арифметика. Модульная арифметика	3
	Применение методов шифрования перестановкой	3
	Применение методов шифрования заменой	2
	Применение методов шифрования многоалфавитной замены	2
	Криптоанализ методов перестановки	2
	Криптоанализ методов замены	
	Компьютерное шифрование	2
Тема 2.2. Современные стандарты шифрования	**Содержание**	**22**
	Симметричное шифрование.	2
	Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES.	2
	Усовершенствованный стандарт шифрования AES.	2
	Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES.	
	Российские стандарты симметричного шифрования .	2
	Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015.	2
	Проблема распределения ключей симметричного шифрования.	2
	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.	2
	Российские стандарты асимметричного шифрования.	2
	ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.	2
	Практические и лабораторные работы	**4**
	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	
	Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	
Тема 2.3. Криптографические методы обеспечения безопасности сетевых	**Содержание**	**66**
	Целостность сообщения.	2
	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.	2

технологий	Электронная цифровая подпись.	2
	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.	2
	Установление подлинности объекта.	2
	Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены.	2
	Проблемы распределения открытого ключа асимметричного шифрования.	2
	Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI.	2
	Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне.	2
	Электронная почта. Архитектура e-mail. PGP. S/M1ME .	2
	Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне.	2
	Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети	2
	Защита информации в сетях организованных по технологии беспроводного доступа.	2
	IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16.	2
	Защита информации в сетях сотовой связи.	2
	A3. A8.A5/3. Атаки на алгоритмы.	2
	Перспективы развития беспроводной мобильной связи.	2
	Криптовалюты.	2
	Биткоин. Блокчейн-системы Ethereum.	2
	Перспективы развития криптографии.	2
	Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.	2
	Практические и лабораторные работы	**24**
	Разработка хэш-функции	2
	Разработка схемы простого пароля	2
	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		**10**
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.	
Курсовой проект (работа)	**30**
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.	
Консультации	*4*
Промежуточная аттестация по МДК.02.02 в форме дифференцированного зачета	*4*
УП.02.01 Учебная практика	**108**

Виды работ:	
Выбор, подключение, настройка межсетевого экрана.	
Администрирование межсетевого экрана.	
Ознакомление, подключение, настройка системы резервного копирования	
Администрирование системы резервного копирования.	
Ознакомление, подключение, настройка системы антивирусной защиты.	
Администрирование системы антивирусной защиты.	
Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции	
Составление алгоритма шифра	
Подключение, установка драйверов, настройка программных средств шифрования Криптон.	
Администрирование программных средств шифрования Криптон	
Консультации	**2**
Промежуточная аттестация по Учебной практике (УП.02.01) в форме дифференцированного зачета	
ПП.02.01 Производственная практика	**72**
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	
Консультации	**2**
Промежуточная аттестация по Производственной практике (ПП.02.01) в форме дифференцированного зачета	
Итоговая аттестация по ПМ.02 в виде Квалификационного экзамена	**8**
Всего по ПМ:	**643**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация рабочей программы профессионального модуля предполагает наличие

лаборатории «Программно-аппаратных средств обеспечения информационной безопасности», «Аппаратных средств вычислительной техники», радиомонтажной мастерской.

Оборудование лаборатории «Программно-аппаратных средств обеспечения информационной безопасности»:

персональные компьютер с аппаратной поддержкой виртуализации и техническими характеристиками не ниже i7\16 Gb \SSD 128\HDD 1 Tb\VGA integrate\ Monitor 23";
программное обеспечение VirtualBox, KVM;

программное обеспечение OpenOffice;
аппаратное обеспечение ISR G2 (Cisco 2901);

аппаратное обеспечение Cisco Catalyst WS-2960+24TC-L;
аппаратное обеспечение Cisco ASA 5505;

СЗИ от НСД DallasLock, SecretNet;
АПКШ «Контитнент»;

специализированное ПО, находящееся в свободном доступе;
проектор;

сетевой лазерный принтер для бумаги форматов А3, А4;
столы и стулья.

Оборудование лаборатории «Аппаратных средств вычислительной техники»:

персональные компьютер с аппаратной поддержкой виртуализации и техническими характеристиками не ниже i7\16 Gb \SSD 128\HDD 1 Tb\VGA integrate\ Monitor 23";
программное обеспечение VirtualBox, KVM ;
программное обеспечение OpenOffice;
персональный компьютер и проектор;

сетевой лазерный принтер для бумаги форматов А3, А4;
столы и стулья.

***3.2.** Информационное обеспечение обучения*

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

Основные источники:

1. Ю.А.Родичев. Нормативная база и стандарты в области информационной безопасности. Учебное пособие - СПб.: Питер, 2017г. – 256 стр.
2. Бутакова, Н.Г. Криптографические методы защиты информации, учебное пособие [Электронный ресурс] : учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. — Электрон. дан. — Санкт-Петербург : ИЦ Интермедия, 2016. — 384 с. — Режим доступа: https://e.lanbook.com/book/90270. — Загл. с экрана.
3. Стеганографические и криптографические методы защиты информации: учебное пособие [Электронный ресурс] : учеб. пособие — Электрон. дан. — Уфа : БГПУ имени

М. Акмуллы, 2016. — 112 с. — Режим доступа: https://e.lanbook.com/book/90963. — Загл. с экрана.

4. Лидовский, В.В. Основы теории информации и криптографии [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : , 2016. — 141 с. — Режим доступа: https://e.lanbook.com/book/100349

5. Аверченков, В.И. Криптографические методы защиты информации: учебное пособие [Электронный ресурс] : учеб. пособие / В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. — Электрон. дан. — Москва : ФЛИНТА, 2017. — 215 с. — Режим доступа: https://e.lanbook.com/book/92914.
6. В.Г. Олифер, Н.А. Олифер "Компьютерные сети. Принципы, технологии, протоколы". 5-е изд., – СПб: Питер, 2017.- 992с.
7. Будылдина Н.В., Шувалов В.П. Сетевые технологии высокоскоростной передачи данных. Учебное пособие для вузов. - 2017 г., - 342 стр. Горячая Линия - Телеком.
8. Олифер В.Г., Олифер Н.А. Безопасность компьютерных сетей. Учебное пособие. - 2017 г., - 644 стр. Горячая Линия - Телеком
9. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – Москва: НТИ «Горячая линия–Телеком». – 2017; - 586стр.
10. Скабцов Н. В. Аудит безопасности информационных систем. Изд. Питер, 2018. – 272стр.
11. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278
12. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. – Москва: НТИ «Горячая линия–Телеком». – 2017; - 338стр

Дополнительные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. 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».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. 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.

11. Положение по аттестации объектов информатизации по требованиям безопасности

информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
13. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
14. 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.
15. 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.
16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
17. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
18. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
19. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
20. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
21. 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.
22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
23. 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
24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
28. 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
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
30. 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
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
38. 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.
39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
40. 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.
41. 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.
42. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
46. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
47. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

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; - проводить конфигурирование программных и программно-аппаратных	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	- 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