ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

АРХАНГЕЛЬСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ
ИМ. Б.Л. РОЗИНГА (ФИЛИАЛ) СПбГУТ
(АКТ (ф) СПбГУТ)

Топанов Александр Павлович

Подписано цифровой подписью: Топанов Александр Павлович

УТВЕРЖДАЮ
Зам. директора по учебной работе
_____ М.А. Цыганкова
3 _____ 2023 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

по специальности:

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

г. Архангельск
2023

Рабочая программа профессионального модуля составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, примерной основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем и в соответствии с учебным планом по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа рассмотрена и одобрена цикловой комиссией Информационной безопасности инфокоммуникационных систем

Протокол № 8 от 31 04 2023 г.

Председатель _____ А.А. Садков

Составитель:

А.А. Садков, преподаватель первой квалификационной категории АКТ (ф) СПбГУТ.

СОДЕРЖАНИЕ

1	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2	СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
3	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	33
4	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	38

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 Область применения рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2 Цель и планируемые результаты освоения профессионального модуля

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

1.2.1 Перечень общих компетенций и личностных результатов реализации программы воспитания

Код	Наименование общих компетенций и личностных результатов
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 языках.
ЛР 1- ЛР 4, ЛР 10, ЛР 13- ЛР 26.	

1.2.2 Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	**Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты**
ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от 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

1.2.3 В результате освоения профессионального модуля студент должен:

Иметь практический опыт	- установки, настройки, испытаний и конфигурирования программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей; - поддержания бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; - защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.
уметь	- 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; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; - проводить установление 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.
знать	-возможные угрозы безопасности информации в ИТКС; - способы защиты информации от несанкционированного доступа (далее-НСД) и специальных воздействий на нее; -типовые программные и программно-аппаратные средства защиты информации и информационно - телекоммуникационных системах и сетях; - криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; - порядок тестирования функций программных и программно – аппаратных, в том числе криптографических средств защиты информации; - организацию и содержание технического обслуживания и ремонта программно – аппаратных, в том числе криптографических средств защиты информации; - порядок и правила ведения эксплуатационной документации на программные и программно – аппаратные, в том числе криптографических средств защиты информации.

1.3 Количество часов, отводимое на освоение профессионального модуля

Всего часов – 746

в том числе в форме практической подготовки – 398.

Из них

на освоение МДК.02.01 – 272 часа, в том числе самостоятельная работа – 32 часа.

МДК.02.02 –168 часов, в том числе самостоятельная работа – 8 час.

на практики – 288 часов, в том числе учебную – 108 часов и производственную – 180 часов.

Промежуточная аттестация – 18 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, ак. час.							
			Работа обучающихся во взаимодействии с преподавателем						Самостоятельная работа	Промежуточная аттестация (экзамен)
			Обучение по МДК				Практики			
			Всего	В том числе						
				Лабораторных и практических занятий	Курсовых работ (проектов)	Зачетные занятия	Учебная	Производственная		
ПК 2.1-2.3 ОК 01-04, ОК 09,10	Раздел 1 Программные, программно-аппаратные методы защиты информации в информационно-телекоммуникационных системах и сетях	**272**	**240**	66	20	2	-	-	**32**	-
ПК 2.1-2.3 ОК 01-04, ОК 09,10	Раздел 2 Криптографические методы защиты информации	**168**	**160**	44	10	2	-	-	**8**	-
ПК 2.1-2.3 ОК 01-04, ОК 09,10	Учебная практика	**108**					**108**	-	-	-
ПК 2.1-2.3 ОК 01-04, ОК 09,10	Производственная практика	**180**						**180**	-	-
ПК 2.1-2.3 ОК 01-04, ОК 09,10	Промежуточная аттестация (экзамен)	**18**						-	-	***18***
	Всего:	***746***	***400***	***110***	***30***	***4***	***108***	***180***	***40***	***18***

2.2 Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)		Объем в часах
Раздел ПМ 1. Программные, программно-аппаратные методы защиты информации в информационно-телекоммуникационных системах и сетях			**452**
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			**452**
Тема 1.1 Обеспечение безопасности операционных систем	**Содержание учебного материала**		**28**
	1	Проблемы обеспечения безопасности операционных систем.	2
	2	Полностью контролируемые системы. Частично-контролируемые системы.	2
	3	Операционные системы на основе ядра NT.	2
	4	Операционные системы на основе ядра Linux.	2
		Операционные системы на основе ядра QNX.	
	5	Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя.	2
	6	Методы аутентификации. Пароли. PIN-коды. Методы надежного составления паролей.	2
	7	Строгая аутентификация. Односторонняя аутентификация. Двухсторонняя аутентификация. Многофакторная аутентификация.	2
	8	Аппаратно-программные средства идентификации и аутентификации. Токены. Смарт-карты. Виртуальные ключи.	2
	9	Идентификации и аутентификации биометрическими методами.	2

	10	Программно-аппаратные модули доверенной загрузки.	2
	11	Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. АПМДЗ Криптон –Замок системный администратор.	2
	12	Изучение настроек системного администратора АПМДЗ. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ.	2
	13	Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ	2
	14	Секторы накопителей на магнитных жестких дисках и твердотельных накопителей. Область памяти. Файл, папка, каталог.	2
	Практические занятия		**10**
	1	Настройка локальной политики безопасности Windows.	2
	2	Настройка изолированной среды	2
	3	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	2
	4	Настройка программные средства шифрования.	2
	5	Восстановление информации типовыми средствами	2
	Лабораторные занятия		**4**
	1	Изучение средств идентификации аутентификации операционных систем	2
	2	Исследование аппаратного средства шифрования настройка, эксплуатация	2
	Самостоятельная работа обучающихся		**8**
	1	Проблемы обеспечения безопасности операционных систем WindowsXP. Windows 7. Windows8. Linux. QNX.	2
	2	Аутентификация, авторизация и администрирование	2

		действий пользователя. Технологии аутентификации.	
	3	Токены. Смарт-карты. Виртуальные ключи.	2
	4	Комплексная система организации управления доступом. Инсталляция. Настройка.	2
Тема 1.2 Технологии разграничения доступа	**Содержание учебного материала**		**46**
	1	Архитектура подсистемы защиты операционной системы редакции Server. Особенности ОС редакции Server.	2
	2	Возможности администратора. Разграничение доступа к объектам операционной системы.	2
	3	Модели доступа. Дискреционная модель. Мандатная модель. Роли.	2
	4	Локальная политика безопасности. Настройка локальной политики безопасности.	2
	5	Администрирование операционной системы. Изолированная программная среда.	2
	6	Способы организации. Методы применения. ActiveDirectory.	2
	7	Доменная политика безопасности. Настройка доменной политики безопасности.	2
	8	Комплексная система организации управления доступом. Инсталяция. Настройка.	2
	9	Аудит безопасности операционной системы.	2
	10	Методы проведения контрольных проверочных мероприятий. Программные средства аудита.	2
	11	Ограничение доступа внешних пользователей. Разграничение доступа.	2
	12	Фильтрация трафика. Анализ информации. Пакетная фильтрация.	2
	13	Функции межсетевых экранов. Посреднические функции.	2

		Дополнительные возможности МЭ.	
	14	Особенности функционирования межсетевых экранов. Модель OSI.	2
	15	Экранирующий маршрутизатор. Шлюз сеансового уровня.	2
	16	Прикладной шлюз. Шлюз экспертного уровня.	2
	17	Схемы защиты на базе межсетевых экранов.	2
	18	Политика межсетевого взаимодействия. Схемы подключения МЭ.	2
	19	Персональные и распределенные МЭ. Проблемы безопасности МЭ.	2
	20	Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ.	2
	21	Требования ФСТЭК к МЭ.	2
	22	Системы уровня L2. Фильтрация на основе Port Security. Безопасность канального уровня.	2
	23	Построение сетей на основе VLAN для разграничения доступа к объектам внутри локальной сети.	2
	Лабораторные занятия		**10**
	3	Анализ программ надежного удаления информации	2
	4	Анализ средств архивирования информации	2
	5	Анализ программных средств резервного копирования. Настройка RAID-массивов	2
	6	Анализ инсайдерской информации. Программы сбора информации о ПК	2
	7	Анализ настройки межсетевого экрана.	2
	Самостоятельная работа обучающихся		**10**
	5	Программно-аппаратные модули доверенной загрузки. Изучение настроек системного администратора АПМДЗ.	2
	6	Разграничение доступа к объектам операционной системы.	2

	7	Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика.	2
	8	Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.	2
	9	Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ.	2
Тема 1.3 Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание учебного материала**		**38**
	1	Проблемы информационной безопасности сетей.	2
	2	Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP.	2
	3	Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности.	2
	4	Пути решения проблем защиты информации в сетях. Концепция построения виртуальных защищенных сетей.	2
	5	Надежная передача информации по незащищенным каналам связи. Шифрование.	2
	6	Аутентификация. Верификация. Избыточное кодирование.	2
	7	VPN – решения для построения защищенных сетей.	2
	8	Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов.	2
	9	Структура пакета. Структура защищенного пакета.	2
	10	Варианты построения защищенных каналов. Классификация.	2
	11	Защита на канальном уровне. Протоколы PPTP, L2F, L2TP.	2
	12	Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS.	2

	13	Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP.	2
	14	Защита на прикладном уровне. DHCP. DNS Sec. HTTPS. Security mail protocol.	2
	15	Организация удаленного доступа. SSH, Telnet, RDP, pop3, imap4, smtp, smb.	2
	16	Управление идентификацией и доступом. Средства управления доступом.	2
	17	Web-доступ. Web-app.	2
	18	Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	2
	19	Wi-fi сети. Bluetooth сети. WPA, WPA-2,WPA-3.	2
	Практические занятия		**20**
	6	Работа с контрольными точками в системах вирутализации	2
	7	Работа с локальным хранилищем сертификатов в ОС WINDOWS	2
	8	Установка и настройка ПО eTokenPKIClient	2
	9	Настройка ПО eTokenPKIClient с помощью групповых политик	2
	10	Развертывание TMS в среде Active Directory	2
	11	Настройка TMS в среде Active Directory	2
	12	Настройка использования виртуального токена	2
	13	Использование токена на рабочем месте администратора	2
	14	Установка и настройка СКЗИ «КриптоПроCSP»	2
	15	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	2
	Лабораторные занятия		**16**
	8	Исследование работы систем виртуализации и с виртуальными машинами	2
	9	Анализ использование внешних устройств в использование	2

		различных систем	
	10	Анализ работы SecretDisk4	2
	11	Анализ работы SecretDisk Server NG	2
	12	Изучение основных возможностей ПО VipNetClient	2
	13	Изучение настроек ПОVipNetClient	2
	14	Изучение возможностей ПО Деловая почта	2
	15	Анализ настройки политик TMS	2
	Самостоятельная работа обучающихся		**8**
	10	Защита на канальном уровне. ПротоколыPPTP, L2F, L2TP.	2
	11	Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS.	2
	12	Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP.	2
	13	Защита на прикладном уровне. ПротоколыPAP, CHAP,S/Key, SSO, Kerberos.	2
Тема 1.4 Технологии обнаружения вторжений	**Содержание учебного материала**		**22**
	1	Технология обнаружения атак. Концепция адаптивного управления безопасностью.	2
	2	Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов.	2
	3	Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.	2
	4	Средства обнаружения сетевых атак. Методы анализа сетевой информации.	2
	5	Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак.	2
	6	Особенности систем обнаружения атак на сетевом и операционном уровнях.	2

	7	Методы реагирования на сетевые атаки.	2
	8	Обзор современных средств обнаружения атак.	2
	9	Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты.	2
	10	Классификация компьютерных вирусов. Жизненный цикл вирусов.	2
	11	Основные каналы распространения вирусов и других вредоносных программ.	2
	Лабораторные занятия		**4**
	16	Изучение средств обнаружения атак	2
	17	Изучение антивирусных продуктов	2
	Самостоятельная работа обучающихся		**2**
	14	Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.	2
Тема 1.5 Методы управления средствами защиты	**Содержание учебного материала**		**18**
	1	Методы управления средствами сетевой защиты.	2
	2	Задачи управления системой сетевой защиты.	2
	3	Архитектура управления средствами сетевой защиты.	2
	4	Функционирование системы управления средствами защиты.	2
	5	Аудит безопасности информационной системы.	2
	6	Мониторинг безопасности системы. Программные средства проведения аудита безопасности.	2
	7	Обзор современных систем управления сетевой защитой.	2
	8	Классификация систем защиты.	2
	9	Перспективы и тенденции в развитии систем защиты.	2
	Лабораторные занятия		**2**
	18	Исследование систем управления средствами централизованной защиты OSSIM	2

	Самостоятельная работа обучающихся		**4**
	15	Функционирование системы управления средствами защиты.	2
	16	Аудит безопасности информационной системы.	2
Курсовое проектирование	**Обязательные аудиторные учебные занятия по курсовому проекту**		**20**
	1	Введение. Выдача заданий.	2
	2	Анализ поставленной задачи.	2
	3	Анализ и выбор возможных решений.	2
	4	Составления перечня этапов разработки.	2
	5	Анализ механизмов защиты.	2
	6	Анализ существующих угроз поставленных задач.	2
	7	Анализ требуемых компонентов.	2
	8	Проектирование модели угроз.	2
	9	Настройка компонентов защиты.	2
	10	Конфигурирование пользовательских задач.	2
Примерная тематика курсовых проектов	**Содержание примерных тем курсовых проектов**		
	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.	
Зачётное занятие			**2**
Учебная практика по разделу 1	**Виды работ**		**72**
	1	Разработка концепции инженерной защиты информации.	2
	2	Построение матрицы технических угроз объекта.	2
	3	Исследование методов и способов несанкционированного съема сигнала.	2
	4	Исследование методов и способов экранирования среды передачи данных.	2
	5	Исследование методов и способов экранирования средств обработки и хранения информации.	2
	6	Разработка модели подсистемы защиты информации от съема сигнала наводки.	2

	7	Разработка модели подсистемы защиты средств обработки информации с применением технологии экранирования	2
	8	Изучение методов и способов создания технических каналов утечки информации.	2
	9	Разработка модели процесса защиты активов от утечки информации по техническим каналам.	2
	10	Разработка плана ввода в эксплуатацию системы инженерно-технической защиты информации объекта.	2
	11	Ознакомление с практическими методами противодействия наблюдению и основными характеристиками средств и систем противодействия наблюдению.	2
	12	Работа со средствами и системами противодействия наблюдению.	2
	13	Ознакомление с методами и способами противодействия процессу утечки информации по акустическому и виброакустическому каналу.	2
	14	Работа со средствами противодействия процессу утечки информации по акустическому и виброакустическому каналу.	2
	15	Ознакомление с методами и средствами перехвата информации и выработка механизмов защиты от перехвата информации.	2
	16	Работа с механизмами защиты среды передачи данных от перехвата информации.	2
	17	Ознакомление со способами реализации охранных систем.	2
	18	Составление концепции управления рисками в области информационной безопасности предприятия.	2
	19	Работа с программными средствами анализа рисков.	2

	20	Составление матрицы угроз для предприятия.	2
	21	Развертывание систем обнаружения вторжений.	2
	22	Конфигурирование систем обнаружения вторжений.	2
	23	Настройка систем обнаружения вторжений для обнаружения сетевых атак.	2
	24	Составление политики безопасности предприятия с учетом работы систем обнаружения вторжений.	2
	25	Тестирования аппаратных межсетевых экранов.	2
	26	Тестирования программных межсетевых экранов.	2
	27	Настройка персональных межсетевых экранов.	2
	28	Настройка и конфигурирование межсетевых экранов в сетях SOHO.	2
	29	Настройка и конфигурирование межсетевых экранов в средних сетях.	2
	30	Моделирование работы межсетевых экранов в крупных сетях.	2
	31	Моделирование защищенных каналов связи в различных сетях.	2
	32	Организация процесса построения защищенных каналов связи в различных сетях.	2
	33	Настройка механизмов защиты файловых систем и баз данных.	2
	34	Настройка различных механизмов защиты электронной почты в сети предприятия.	2
	35	Моделирование подсистем обеспечения безопасности информации от несанкционированного доступа.	2
	36	Ознакомление, подключение, настройка системы резервного копирования	2

Производственная практика раздела 1	**Виды работ**		**108**
	1	Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда.	
	2	Выявление угроз безопасности информации на защищаемом объекте.	
	3	Оценка угроз безопасности информации на защищаемом объекте.	
	4	Выявление возможных технических каналов утечки информации на защищаемом объекте.	
	5	Оценка возможностей утечки информации по техническим каналам на защищаемом объекте.	
	6	Применение технических методов защиты информации на защищаемом объекте.	
	7	Применение технических средств защиты информации на защищаемом объекте.	
	8	Использование средств охраны объектов.	
	9	Использование средств безопасности охраны объектов.	
	10	Использование средств инженерной защиты на защищаемом объекте.	
	11	Использование средств технической охраны на защищаемом объекте.	
	12	Осуществление установки технических средств защиты информации на защищаемом объекте.	
	13	Осуществление настройки технических средств защиты информации на защищаемом объекте.	
	14	Осуществление обслуживания технических средств защиты информации на защищаемом объекте.	
	15	Осуществление установки средств охраны на защищаемом объекте.	

	16	Решение частных технических задач при аттестации средств на защищаемом объекте.	
	17	Решение частных технических задач при аттестации средств обеспечения безопасности на защищаемом объекте.	
	18	Решение частных технических задач при аттестации помещений на защищаемом объекте.	
	19	Осуществление настройки оборудования средств защиты на защищаемом объекте.	
	20	Осуществление регулировки оборудования средств защиты на защищаемом объекте.	
	21	Осуществление профилактических работ для оборудования средств защиты на защищаемом объекте.	
	22	Осуществление настройки средств охраны на защищаемом объекте.	
	23	Осуществление обслуживания средств охраны на защищаемом объекте.	
	24	Разработка рекомендаций по внедрению технических средств защиты на защищаемом объекте.	
	25	Выделение на предприятии помещений участвующих в процессах хранения защищаемой информации.	
	26	Выделение на предприятии помещений, участвующих в процессах обработки защищаемой информации.	
	27	Выделение на предприятии помещений участвующих в процессах доступа к защищаемой информации.	
	28	Использование правовой документации в области защиты информации ограниченного доступа.	
	29	Использование нормативных документов в области защиты информации ограниченного доступа.	

	30	Участие в работах по обеспечению безопасности выделенных помещений, обрабатывающих конфиденциальную информацию.	
	31	Участие в работах по проектированию, внедрению и эксплуатации выделенных помещений, обрабатывающих конфиденциальную информацию.	
	32	Участие в работах по проектированию, внедрению и эксплуатации рабочих мест, обрабатывающих конфиденциальную информацию.	
	33	Участие в работах по проектированию средств анализа элементов безопасности рабочих мест, обрабатывающих конфиденциальную информацию.	
	34	Участие в работах по внедрению средств анализа элементов безопасности рабочих мест, обрабатывающих конфиденциальную информацию.	
	35	Участие в работах по эксплуатации средств анализа элементов безопасности рабочих мест, обрабатывающих конфиденциальную информацию.	
	36	Участие в работах по проектированию средств анализа элементов безопасности помещений, обрабатывающих конфиденциальную информацию.	
	37	Участие в работах внедрению средств анализа элементов безопасности помещений, обрабатывающих конфиденциальную информацию.	
	38	Участие в работах по эксплуатации средств анализа элементов безопасности помещений, обрабатывающих конфиденциальную информацию.	
	39	Участие в работах по проектированию средств контроля элементов безопасности помещений, обрабатывающих	

		конфиденциальную информацию.	
	40	Участие в работах по внедрению средств контроля элементов безопасности помещений, обрабатывающих конфиденциальную информацию.	
	41	Участие в работах по эксплуатации средств контроля элементов безопасности помещений, обрабатывающих конфиденциальную информацию.	
	42	Участие в работах по проектированию средств контроля элементов безопасности рабочих мест, обрабатывающих конфиденциальную информацию.	
	43	Участие в работах по внедрению средств контроля элементов безопасности рабочих мест, обрабатывающих конфиденциальную информацию.	
	44	Участие в работах эксплуатации средств контроля элементов безопасности рабочих мест, обрабатывающих конфиденциальную информацию.	
	45	Участие в работах по проектированию средств безопасности помещений и рабочих мест, обрабатывающих конфиденциальную информацию.	
	46	Участие в работах внедрению средств безопасности помещений и рабочих мест, обрабатывающих конфиденциальную информацию.	
	47	Участие в работах реализации средств безопасности помещений и рабочих мест, обрабатывающих конфиденциальную информацию.	
	48	Проведение типовых операций настройки средств защиты операционных систем для помещений, обрабатывающих конфиденциальную информацию.	
	49	Участие в работах по обеспечению безопасности	

		выделенных рабочих мест, обрабатывающих конфиденциальную информацию.	
	50	Организация безопасного доступа к информационным ресурсам информационно-телекоммуникационной системы: проведение установки программно-аппаратных средств защиты информации.	
	51	Проведение типовых операций настройки средств защиты операционных систем для рабочих мест, обрабатывающих конфиденциальную информацию.	
	52	Организация безопасного доступа к информационным ресурсам информационно-телекоммуникационной системы: проведение настройки типовых программно-аппаратных средств защиты информации.	
	53	Обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств.	
	54	Обобщение материала, оформление отчета.	
Раздел ПМ 2. Криптографические методы защиты информации			**276**
МДК 02.02.Криптографическая защита информации			**276**
Тема 2.1. Основы криптографических методов защиты информации	**Содержание учебного материала**		**30**
	1	Свойства информационной безопасности.	2
	2	Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации.	2
	3	Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности.	2
	4	Криптографические методы. Шифрование. Кодирование. Стеганография.	2
	5	Сжатие. Математика криптографии.	2
	6	Бинарные операции. Арифметика целых чисел.	2

	7	Модульная арифметика. Матрицы.	2
	8	Линейное сравнение. Традиционные шифры перестановки.	2
	9	Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры.	2
	10	Механизация шифрования. Традиционные шифры замены.	2
	11	Шифры замены. Шифры многоалфавитной замены. Частотность символов.	2
	12	Криптоанализ. Атака грубой силы. Частотный анализ.	2
	13	Атака по образцу. Атака знания исходного текста .	2
	14	Компьютерное шифрование. Кодовая таблица ASCII.	2
	15	Алгебраические структуры: группы, кольца, поля. Генератор паролей.	2
	Практические занятия		**10**
	1	Применение методов шифрования перестановкой	2
	2	Применение методов шифрования заменой	2
	3	Применение методов шифрования многоалфавитной замены	2
	4	Применение компьютерного шифрования	2
	5	Применение стеганографических методов скрытия информации	2
	Лабораторные занятия		**6**
	1	Анализ бинарной арифметики. Модульная арифметика	2
	2	Анализ методов криптоанализа перестановки	2
	3	Анализ методов криптоанализа замены	2
	Самостоятельные работы		**2**
	1	Атака знания исходного текста.	2
Тема 2.2. Современные стандарты шифрования	**Содержание учебного материала**		**32**
	1	Симметричное шифрование. Сети Файстеля.	2
	2	Стандарт шифрования данных DES. Структура DES.	2

	3	Анализ DES. Многократное применение DES. Безопасность DES.	2
	4	Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256.	2
	5	Анализ безопасности AES.	2
	6	Российские стандарты симметричного шифрования. Структура ГОСТ 28147-89.	2
	7	Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015.	2
	8	Проблема распределения ключей симметричного шифрования.	2
	9	Алгоритм Диффи-Хелмана. Управление ключами. Kerberos.	2
	10	Асимметричное шифрование. Простые числа и уравнения.	2
	11	Разложение на множители. RSA. Теорема об остатках.	2
	12	Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля.	2
	13	Криптосистемы на основе метода эллиптических кривых. ЭЦП.	2
	14	Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001	2
	15	Российские стандарты асимметричного шифрования ГОСТ Р 34.10 -2012.	2
	16	Безопасность асимметричных алгоритмов.	2
	Лабораторные занятия		**4**
	4	Исследование алгоритма Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	2
	5	Исследование Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на	2

		множители	
	Самостоятельная работа обучающихся		**6**
	2	Стандарт шифрования данных DES.	2
	3	Управление ключами, используя Kerberos.	2
	4	Асимметричное шифрование ГОСТ Р 34.10 -2012.	2
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	**Содержание учебного материала**		**42**
	1	Целостность сообщения. Случайная модель Огас1е. Установление подлинности сообщения.	2
	2	Криптографические хэш-функции. MD-5. SHA-1. SHA-512.	2
	3	ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012	2
	4	Анализ безопасности хэш-функций. Атаки на хэш-функции.	2
	5	Электронная цифровая подпись. Алгоритм формирования подписи.	2
	6	Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись.	2
	7	ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012.	2
	8	Установление подлинности объекта. Простой пароль. Динамический пароль. Запрос-ответ.	2
	9	PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации.	2
	10	Электронные ключи и карты. Токены.	2
	11	Проблемы распределения открытого ключа асимметричного шифрования.	2
	12	Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI.	2
	13	Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне.	2

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

	7	Исследование настройки сервисов Рутокен-ЭЦП	2
	8	Исследование настройки сервисов Рутокен–Bluetooth	2
	9	Исследование настройки сервисов Рутокен–S	2
	10	Анализ разработки алгоритма PGP	2
Курсовое проектирование	**Обязательные аудиторные учебные занятия по курсовому проекту**		**10**
	1	Конфигурирование системы защиты.	2
	2	Подготовка проекторной документации.	2
	3	Внедрение проекта.	2
	4	Тестирование проекта.	2
	5	Защита курсового проекта.	2
Зачётное занятие			**2**
Учебная практика по разделу 2	**Виды работ**		**36**
	1	Конфигурирование шифрующей файловой системы EFS	2
	2	Создание подписей и сертификатов, шифрование документов при помощи EFS.	2
	3	Конфигурирование СКЗИ крипто АРМ	2
	4	Создание подписей и сертификатов, шифрование документов при помощи крипто АРМ.	2
	5	Подписывание объектов с помощью АРМ	2
	6	Конфигурирование СКЗИ GnuPG	2
	7	Подписывание объектов с помощью GnuPG	2
	8	Конфигурирование СКЗИ PGP	2
	9	Подписывание объектов с помощью PGP	2
	10	Конфигурирование СКЗИ TrueCrypt. Шифрование разделов и дисков при помощи TrueCrypt	3
	11	Конфигурирование SSL на операционной системе DEBIAN	3
	12	Конфигурирование SSH на операционной системе DEBIAN	3

	13	Установка и конфигурирование центра сертификации на DEBIAN	3
	14	Создание и перенос контейнеров на Crypto PRO, Конфигурирование считывателей	2
	15	Создание электронных подписей и сертификатов при помощи Crypto PRO	2
	16	Создание запросов и получение сертификатов центра сертификации windows server	2
Производственная практика по разделу 2	**Виды работ**		**72**
	1	Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда.	
	2	Использование методов шифрования для подписи документов.	
	3	Пользование терминологией современной криптографии	
	4	Использование типовых криптографических средств защиты информации	
	5	Использование методов шифрования для писем документов.	
	6	Использование методов шифрования для подписи файлов.	
	7	Использование методов шифрования для шифрования пользовательских папок.	
	8	Использование методов шифрования для шифрования архивов и backup - данных.	
	9	Использование методов шифрования для защиты передаваемой информации по каналам связи.	
	10	Настройка средств электронной подписи	
	11	Администрирование средств электронной подписи	
	12	Администрирование средств PKI	
	13	Обобщение материала, оформление отчета.	

Промежуточная аттестация (экзамен)	**18**
Всего	**746**

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Реализация программы модуля требует наличия лаборатории защиты информации от утечки по техническим каналам, лаборатории программных и программно-аппаратных средств защиты информации, лаборатории информационно-телекоммуникационных систем и сетей, Мастерской по компетенции «Кибер-безопасность».

Лаборатория защиты информации от утечки по техническим каналам, оснащенная оборудованием и техническими средствами обучения: доска классная – 1 шт., стол компьютерный– 13 шт., стул – 13 шт., компьютерные кресла – 13 шт., системный блок (CPU AMD Ryzen 7 3700x (8 Cores/32MB/8T/3.6GHz); 16 Гбайт (16 Гбайт) памяти DDR4, 2 666 МГц, без ECC; твердотельный накопитель M.2 PCIe NVMe, 512 Гбайт, класс 35) – 13 шт., монитор (Asus 23”8) – 13 шт., клавиатура (Oklick 530S) – 14 шт., мышь для компьютера (Defender OPTICAL MB-160) – 14 шт., источник бесперебойного питания – 13 шт., проектор – 1 шт., активная колонка - 1шт., офисный пакет Microsoft Office Professional 2016 - 13 шт, виртуальный межсетевой экран следующего поколения Cisco Firepower в составе с FMC- 10 шт., ОС Microsoft Windows Server - 1 шт., ОС Microsoft Windows 10 - 13 шт., сервер SuperMicro CSE-113AC2-R706WB2 2x750W black Intel Xeon Silver 4216 256 ГБ ОЗУ, 960 GB SSD - 1 шт., монитор 23,6 – 1 шт., источник бесперебойного питания для сервера - 1 шт., стойка двухрамная (стк-24.2-9005 цмо) – 1 шт., телевизор на стойке (huawei 55”) – 1 шт., экран для проектора (SAKURA CINEMA WALLSCREEN) – 1 шт., МФУ (Xerox B205) – 1 шт., ПАК Arduino - 3 шт.,Анализатор спектра IFR 2398 - 1 шт.,Электронный осциллограф IBIS-1 — 1шт.,Соболь 3.0 kb-sobol 3.0 k1 v1-SP1Y - 2 шт .,Видео регистратор jassun jsr-H0415mini - 1 шт.,Видео регистратор vesta VDRV-5004M - 1 шт.,Коммутатор Alcatel OmniStack LS 6224 - 5 шт .,Программные межсетевые экраны для маршрутизаторов Cisco 1700 (Cisco 1721) - 2 шт.,Стенд : пульт защиты помещений — 1 шт.,Стенд: исследование утечки информации по звуковым каналам — 1 шт., стойки для монтажа сетевого оборудования - 2 шт. Программное обеспечение: MS Windows Server 2008 R2, OS Debian Linux 9, Audacity 2.3, Zoneminder 1.32, Open VAS 8, LibreOffice 6, OS Ubuntu Linux 14.04, Virtual Box 5, Open SSL 1.0, Open VPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2, Ossec 3.2, IredMail 0.9.9, OS FreeBSD 11,12. Asterisk 13, PHP MyAdmin 5, Wireshark 2.2.6, Zenmap 7.7, Platinum Pack 4.0., Eset Nod32 Fire Wall 5.,Крипто Про.,RedCheck 2.0.,DevieeLock 8.

Стол преподавателя на металлокаркасе -1шт., кресло Юпитер -2шт., стол компьютерный на металлокаркасе левый- 4шт., стол компьютерный на металлокаркасе правый -10шт., стол на металлокаркасе- 1шт., стул СМ-9ГП-14шт., табурет СМ-31- 14шт., тележка под системный блок- 1шт., рабочее место

преподавателя – ПК -1 шт: Монитор 19” TFT LG Flatron L1942SE-BF -1 шт., Foxconn TSAA-700 (Корпус)-1 шт., ASRock H67DE3 (Материнская плата)-1 шт., Intel HD Graphics (Видеокарта)-1 шт., Realtek PCIe GBE (Сетевая плата)-1 шт., Realtek HDA (Звуковая плата)-1 шт., Intel Core i3 2120 3.3GHz (Процессор)-1 шт., 4xDDR III 2Gb Samsung (ОЗУ)-1 шт., D-Link DGE-528T (Сетевая плата)-1 шт, WD (500Gb) SATA III (Жесткий диск)-1 шт.,рабочие места обучающихся – ПК 14 шт: монитор 19” TFT LG Flatron L1942SE-BF - 14 шт, Foxconn TSAA-700 (Корпус)- 14 шт,ASRock H67DE3 (Материнская плата)- 14 шт, Intel HD Graphics (Видеокарта)- 14 шт, Realtek PCIe GBE (Сетевая плата)- 14 шт, Realtek HDA (Звуковая плата)- 14 шт, Intel Core i3 2120 3.3GHz (Процессор)- 14 шт, 4xDDR III 2Gb Samsung (ОЗУ)- 14 шт,D-Link DGE-528T (Сетевая плата) - 14 шт, WD (500Gb) SATA III (Жесткий диск)- 14 шт, мультимедиа-проектор (Epson EB-X12),- 1шт, экран (Screen Media GoldView MW),- 1 шт, учебная доска -1шт., маршрутизатор D-Link Dir-320-1шт., маршрутизатор D-Link DSR-500N-1шт., маршрутизатор D-link DFL-800- 1шт., коммутатор D-Link DGS-3312SR – 2шт., коммутатор D-Link DES-3528 – 8шт., стойка для монтажа сетевого оборудования – 2 шт., патч-панель – 2шт., клещи обжимные – 8шт., розетки распределительные под RJ-45 – 4шт., конекторы RJ-45 –50шт. Программное обеспечение: MS Windows Server 2008 R2, MS Windows Server 2012 R2, MS Windows Server 2016, OpenVAS 8, LibreOffice 6, ОС Ubuntu Linux 14.04, VirtualBox 5, OpenSSL 1, OpenVPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2.0.2, Ossec 3.2, IredMail 0.9.9, PhpMyAdmin 5, Wireshark 2.2.6, Zenmap 7.70, Denver 3, MySQL Workbench 6.3, Joomla 2, Notepade++ 4.0.2, GNU PG 2.ail, Packet tracer.

Лаборатория программных и программно-аппаратных средств защиты информации, оснащенная оборудованием и техническими средствами обучения: доска классная – 1 шт., стол компьютерный– 13 шт., стул – 13 шт., компьютерные кресла – 13 шт., системный блок (CPU AMD Ryzen 7 3700x (8 Cores/32MB/8T/3.6GHz); 16 Гбайт (16 Гбайт) памяти DDR4, 2 666 МГц, без ECC; твердотельный накопитель M.2 PCIe NVMe, 512 Гбайт, класс 35) – 13 шт., монитор (Asus 23”8) – 13 шт., клавиатура (Oklick 530S) – 14 шт., мышь для компьютера (Defender OPTICAL MB-160) – 14 шт., источник бесперебойного питания – 13 шт., проектор – 1 шт., активная колонка - 1шт., офисный пакет Microsoft Office Professional 2016 - 13 шт, виртуальный межсетевой экран следующего поколения Cisco Firepower в составе с FMC- 10 шт., ОС Microsoft Windows Server - 1 шт., ОС Microsoft Windows 10 - 13 шт., сервер SuperMicro CSE-113AC2-R706WB2 2x750W black Intel Xeon Silver 4216 256 ГБ ОЗУ, 960 GB SSD - 1 шт., монитор 23,6 – 1 шт., источник бесперебойного питания для сервера - 1 шт., стойка двухрамная (стк-24.2-9005 цмо) – 1 шт., телевизор на стойке (huawei 55”) – 1 шт., экран для проектора (SAKURA CINEMA WALLSCREEN) – 1 шт., МФУ (Xerox B205) – 1 шт., ПАК Arduino - 3 шт.,Анализатор спектра IFR 2398 - 1 шт.,Электронный осциллограф IBIS-1 — 1шт.,Соболь 3.0 kb-sobol 3.0 k1 v1-SP1Y - 2 шт .,Видео регистратор jassun jsr-H0415mini - 1 шт.,Видео регистратор vesta VDRV-5004M - 1 шт.,Коммутатор Alcatel OmniStack LS 6224 - 5 шт .,Программные межсетевые экраны для

маршрутизаторов Cisco 1700 (Cisco 1721) - 2 шт.,Стенд : пульт защиты помещений — 1 шт.,Стенд: исследование утечки информации по звуковым каналам — 1 шт., стойки для монтажа сетевого оборудования - 2 шт. Программное обеспечение: MS Windows Server 2008 R2, OS Debian Linux 9, Audacity 2.3, Zoneminder 1.32, Open VAS 8, LibreOffice 6, OS Ubuntu Linux 14.04, Virtual Box 5, Open SSL 1.0, Open VPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2, Ossec 3.2, IredMail 0.9.9, OS FreeBSD 11,12. Asterisk 13, PHP MyAdmin 5, Wireshark 2.2.6, Zenmap 7.7, Platinum Pack 4.0., Eset Nod32 Fire Wall 5.,Крипто Про.,RedCheck 2.0.,DevieeLock 8.

Лаборатории информационно-телекоммуникационных систем и сетей оснащенная оборудованием и техническими и программными средствами обучения: стол аудиторный - 6 шт., стол квадратный - 3 шт., стол однотумбовый - 1 шт., стол компьютерный - 1 шт., стол угловой - 1 шт., стол рабочий - 1 шт., табурет - 18 шт., доска классная - 1 шт., сотовый телефон Samsung GT-S5830 - 1 шт., базовый аппарат Siemens Gigaset4010 Classic - 1 шт., точка доступа D-Link AirPlus Xtreme G DWL-AP2100 - 1 шт., маршрутизатор D-Link DIR-620 - 1 шт., радиоудлинитель - 1 шт., система радиомониторинга ИКАР-2 - 1 шт., радиоприемное устройство icom ic 8500 - 1 шт., прибор В6-9 - 1 шт., прибор ВО-71 - 1 шт., прибор Г3-111 - 1 шт., прибор Г4-102 - 4 шт., прибор Г4-102А - 1 шт., прибор С1-73 - 2 шт., прибор С1-77 - 1 шт., прибор Ч3-33 - 4 шт., прибор В3-38 - 3 шт., прибор 4323 - 2 шт., прибор В7-26 - 1 шт., прибор Ц-4315 - 2 шт., приемник Катран - 7 шт., частотомер Ч3-33 - 1 шт., радиостанция Нива-М - 1 шт., ПК 7 шт: монитор 17” TFT LG Flatron L1730S, системный блок (Microlab/GA-8I865GVME/Intel Celeron D-320 2.4GHz/ 2xDDR 512 Mb| WD Seagate Barracuda 80Gb ,программное обеспечение: Windows XP, LibreOffice 5, Foxit Reader 7, ONEPLAN RPLS-DB, локальная сеть с доступом к ЭБС и СДО.

Мастерская по компетенции «Кибер-безопасность», оснащенная оборудованием и техническими и программными средствами обучения: доска классная – 1 шт., стол компьютерный– 13 шт., стул – 13 шт., компьютерные кресла – 13 шт., системный блок (CPU AMD Ryzen 7 3700x (8 Cores/32MB/8T/3.6GHz); 16 Гбайт (16 Гбайт) памяти DDR4, 2 666 МГц, без ECC; твердотельный накопитель M.2 PCIe NVMe, 512 Гбайт, класс 35) – 13 шт., монитор (Asus 23”8) – 13 шт., клавиатура (Oklick 530S) – 14 шт., мышь для компьютера (Defender OPTICAL MB-160) – 14 шт., источник бесперебойного питания – 13 шт., проектор – 1 шт., активная колонка - 1шт., офисный пакет Microsoft Office Professional 2016 - 13 шт, виртуальный межсетевой экран следующего поколения Cisco Firepower в составе с FMC- 10 шт., ОС Microsoft Windows Server - 1 шт., ОС Microsoft Windows 10 - 13 шт., сервер SuperMicro CSE-113AC2-R706WB2 2x750W black Intel Xeon Silver 4216 256 ГБ ОЗУ, 960 GB SSD - 1 шт., монитор 23,6 – 1 шт., источник бесперебойного питания для сервера - 1 шт., стойка двухрамная (стк-24.2-9005 цмо) – 1 шт., телевизор на стойке (huawei 55”) – 1 шт., экран для проектора (SAKURA CINEMA WALLSCREEN) – 1 шт., МФУ (Xerox B205) – 1 шт., ПАК Arduino - 3

шт.,Анализатор спектра IFR 2398 - 1 шт.,Электронный осциллограф IBIS-1 — 1шт.,Соболь 3.0 kb-sobol 3.0 k1 v1-SP1Y - 2 шт .,Видео регистратор jassun jsr-H0415mini - 1 шт.,Видео регистратор vesta VDRV-5004M - 1 шт., коммутатор Alcatel OmniStack LS 6224 - 5 шт .,Программные межсетевые экраны для маршрутизаторов Cisco 1700 (Cisco 1721) - 2 шт., стенд : пульт защиты помещений — 1 шт., стенд: исследование утечки информации по звуковым каналам — 1 шт., стойки для монтажа сетевого оборудования - 2 шт.

Программное обеспечение: MS Windows Server 2008 R2, OS Debian Linux 9, Audacity 2.3, Zoneminder 1.32, Open VAS 8, LibreOffice 6, OS Ubuntu Linux 14.04, Virtual Box 5, Open SSL 1.0, Open VPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2, Ossec 3.2, IredMail 0.9.9, OS FreeBSD 11,12. Asterisk 13, PHP MyAdmin 5, Wireshark 2.2.6, Zenmap 7.7, Platinum Pack 4.0., Eset Nod32 Fire Wall 5.,Крипто Про.,RedCheck 2.0.,DevieeLock 8.

3.2 Информационное обеспечение реализации программы

3.2.1. Основные печатные и электронные издания:

1. Баранова. Е. К. Моделирование системы защиты информации: Практикум / Е.К. Баранова, А.В. Бабаш. - Москва : ИЦ РИОР, 2018. - 224 с. - ISBN 978-5-369-01559-9. - URL: https://ibooks.ru/reading.php?productid=361422 - – Режим доступа: для зарегистрир.пользователей. - Текст : электронный.

2. Бубнов, А. А. Основы информационной безопасности (3-е изд.) : учебник / А.А. Бубнов. - Москва: Академия, 2020.

3. Бубнов, А.А. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник / Бубнов, А.А. - Москва: Академия, 2019.

4. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-16-104336-3. - URL: https://new.znanium.com/catalog/product/1082470 - Режим доступа: для зарегистр. пользователей. – Текст электронный.

5. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты объекта: учебник / В.П. Зверева, А.В. Назаров. — Москва: КУРС: ИНФРА-М, 2020. — 320 с. - ISBN 978-5-16-105204-4. - URL: https://new.znanium.com/catalog/product/1055808 - Режим доступа: для зарегистр. пользователей. – Текст электронный.

6. Ильин, М.Е. Криптографическая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник. / М.Е. Ильин. - Москва: Академия, 2020.

7. Казарин, О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для СПО / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020.

8. Мельников Д.А. Информационная безопасность открытых систем / Д.А. Мельников. - Москва : Флинта, 2019. - 444 с. - ISBN 978-5-9765-1613-7. - URL: https://ibooks.ru/reading.php?productid=340843 - Режим доступа: для зарегистр. пользователей. – Текст электронный.

9. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - URL: https://znanium.com/catalog/product/1081318. – Режим доступа: для зарегистрир.пользователей. - Текст : электронный.

10. Хорев, П.Б. Программно-аппаратная защита информации / П.Б. Хорев. - Москва : Форум, 2019. - 352 с. - ISBN 978-5-00091-709-1. - URL: https://ibooks.ru/reading.php?productid=361548 - Режим доступа: для зарегистр. пользователей. – Текст электронный.

3.2.2. Дополнительные источники:

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. - Москва: Юрайт, 2020. -URL: https://urait.ru/book/kriptograficheskaya-zaschita-informacii-simmetrichnoeshifrovanie-437667 - Режим доступа: для зарегистр. пользователей. – Текст электронный.

2. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - URL: https://znanium.com/catalog/product/1191479 . – Режим доступа: для зарегистрир.пользователей. - Текст : электронный.

3. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов/ О.И.Шелухин, Д.Ж.Сакалема, А.С.Филинова. - Москва: Горячая линия-Телеком, 2018.- URL: https://ibooks.ru/bookshelf/334051/reading. - Режим доступа: для зарегистр. пользователей. – Текст электронный.

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты	– оценка результатов выполнения практических работ по МДК 02.01 по теме 1.1 №№1-5, по теме 1.3 №№6-15, по МДК 02.02 по теме 2.1 №№1-5, по теме 2.3 №№6-12; - оценка результатов выполнения лабораторных работ по МДК 02.01 по теме 1.1 №№1,2; по теме 1.2 №№3-7, по теме 1.3 №№8-15 по теме 1.4 №№16,17, по теме 1.5 №18; по МДК 02.02 по теме 2.1 №№1-3; по теме 2.2 №№4,5, по теме 2.3 №№6-10 - экспертное наблюдение выполнения лабораторных работ, – экспертное наблюдение выполнения практических работ, - оценка решения ситуационных задач; – оценка результатов выполнения самостоятельной работы;
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	- 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;	– оценка процесса и результатов выполнения видов работ на практике –экзамен
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	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение за выполнением работ –экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические	

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

	Промежуточная аттестация: **МДК.02.01 – ---, дифференцированный зачет** **МДК.02.02 - ---, дифференцированный зачет** **УП.02 - ---, дифференцированный зачет** **ПП.02 - дифференцированный зачет** **ПМ.02 - экзамен по модулю**