Приложение II.2

к программе СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

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

2019

Составитель:

Арефьев Александр Валерьевич, преподаватель ГБПОУ УКРТБ

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

название профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

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

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК10	Пользоваться профессиональной документацией на государственном и иностранном языке.

Код	Наименование видов деятельности и профессиональных компетенций
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 и 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.

В результате освоения профессионального модуля студент должен:

Иметь	Установке, настройке, испытаниях и конфигурировании программных и

практический опыт в	программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей; Поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; Защите 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 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 *Проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации российского производства;* *Проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации российского производства.*
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 средств защиты информации в 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 криптографические средства защиты информации; *Программные и программно-аппаратные средства защиты информации в ИТКС российского производства;* *Криптографические средства защиты информации конфиденциального характера, которые применяются в ИТКС на основе российских стандартов* *Порядок и правила ведения документации планово предупредительных работ*

	на программные и программно-аппаратные (в том числе криптографические) средства защиты информации;

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов – 715 час, в том числе:

- 108 часов вариативной части, направленных на усиление обязательной части программы профессионального модуля.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Суммарный объем нагрузки, час	Объем профессионального модуля, час						
			Обучение по МДК				Практика		Промежуточная аттестация
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Самостоятельная работа	Учебная, часов	Производственная (по профилю специальности), часов	
1	2	3	4	5	6	7	8	9	10
ПК 2.1-ПК 2.3	**Раздел 1.** Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	**273**	**244**	112	20	**17**	**-**	*****	**12**
ПК 2.1-ПК 2.3	**Раздел 1.** Криптографическая защита информации	**184**	**162**	76	10	**14**			**8**
ПК 2.1-ПК 2.3	**Учебная практика**	**108**					**108**		
ПК 2.1-ПК 2.3	**Производственная практика**	**144**						**144**	
	Промежуточная аттестация (экзамен (квалификационный))	**6**							**6**
	Всего:	**715**	**406**	188	**30**	**31**	**108**	**144**	**26**

*Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

2.2. Содержание обучения по профессиональному модулю (ПМ)

IV семестр

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. Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			
МДК.2.1Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			**258**
Тема 1.1 Обеспечение безопасности операционных систем	**Содержание**		**16**
	1	**Проблемы обеспечения безопасности операционных систем**. Полностью контролируемые системы. Частично-контролируемые системы. Windows XP. Windows 7. Windows8. Linux. QNX и другие операционные системы.	2
	2	**Технологии аутентификации** Аутентификация, авторизация и администрирование действий пользователя.	2
	3	**Методы аутентификации** Пароли. PIN-коды. Методы надежного составления паролей.	2
	4	**Строгая аутентификация** Односторонняя аутентификация. Двухсторонняя аутентификация	2
	5	**Аппаратно-программные средства идентификации и аутентификации** Токены. Смарт-карты. Виртуальные ключи.	2
	6	**Программно-аппаратные модули доверенной загрузки** Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ.	2
	7	**АПМДЗ Криптон –Замок системный администратор** Изучение настроек системного администратора АПМДЗ	2
	8	**АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ**	2

		Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ Сектор НЖМД. Область памяти. Файл, папка, каталог.	
	Практические занятия		**16**
	1	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя	
	2	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	
	3	Настройка изолированной среды	
	4-5	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	
	6	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация	
	7	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	
	8	Восстановление информации типовыми средствами Программы восстановление информации	
Тема 1.2 Технологии разграничения доступа	**Содержание**		**20**
	1	**Архитектура подсистемы защиты операционной системы Windows7** Особенности ОС Windows7. Возможности администратора.	2
	3	**Разграничение доступа к объектам операционной системы** Модели доступа. Дискреционная модель. Мандатная модель. Роли.	2
	4	**Локальная политика безопасности** Настройка локальной политики безопасности. Администрирование системы.	2
	5	**Изолированная программная среда** Способы организации. Методы применения.	2
	6	**Active Directory** Комплексная система организации управления доступом. Инсталляция. Настройка	2
	7	**Аудит безопасности операционной системы** Методы проведения контрольных проверочных мероприятий. Программные средства аудита.	2
	8	**Функции межсетевых экранов** Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.	2

	9	**Особенности функционирования межсетевых экранов** Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня.	2
	10	**Схемы защиты на базе межсетевых экранов** Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ.	2
	Практические занятия		20
	1	Программы надежного удаления информации	
	2	Архивирование информации	
	3	Программные средства резервного копирования. Настройка RAID-массивов	
	4	Инсайдерская информация. Программы сбора информации о ПК	
	5	Установка и настройка Active Directory	
	6	Установка и настройка Active Directory	
	7	Установка и настройка Active Directory	
	8	Настройка межсетевого экрана.	
	9	Настройка межсетевого экрана.	
	10	Настройка межсетевого экрана.	
Тема 1.3 **Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN**	**Содержание**		**24**
	1	**Проблемы информационной безопасности сетей** Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP.	2
	2	**Обеспечение информационной безопасности сетей** Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях.	2
	3	**Концепция построения виртуальных защищенных сетей** Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование.	2
	4	**VPN – решения для построения защищенных сетей** Виртуальные защищенные сети. Туннелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация.	2
	5	**Защита на канальном уровне** Протоколы PPTP, L2F, L2TP	4
	6	**Протоколы формирования защищенных каналов на сеансовом уровне**	4

		Протоколы SSL, TLS, SOCKS	
	7	**Защита на сетевом уровне** Архитектура средств безопасности IPSec, AH, ESP.	4
	8	**Защита на прикладном уровне** Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	4
	Практические занятия		24
	1	Работа с локальным хранилищем сертификатов в ОС WINDOWS	2
	2	Установка и настройка ПО eToken PKI Client	2
	3	Настройка ПО eToken PKI Client с помощью групповых политик	2
	4	Развертывание TMS в среде Active Directory	2
	5	Настройка TMS в среде Active Directory. Настройка политик TMS	2
	6	Настройка использования виртуального токена	2
	7	Использование токена на рабочем месте администратора	2
	8	Установка и настройка СКЗИ «КриптоПро CSP»	2
	9	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	2
	10	Применение SecretDisk4. Применение SecretDisk Server NG	2
	11	Изучение основных возможностей ПО VipNet Client Изучение настроек ПОVipNet Client	2
	12	Изучение возможностей ПО Деловая почта	2
Самостоятельная работа при изучении раздела ПМ.2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя. Оформление практических работ, отчетов и подготовка к их защите.			8
Примерная тематика домашних заданий			
1.1.	1 Чтение и анализ литературы:[3]с.223-229 2 Чтение и анализ литературы:[3]с.172-176 3 Чтение и анализ литературы:[3] с.176-186 4 Чтение и анализ литературы:[3] с.188-196 5 Чтение и анализ литературы:[8] с. 1-7 6 Чтение и анализ литературы:[8] с.11-49 7 Чтение и анализ литературы:[8] с.50-58 8 Чтение и анализ литературы:[8] с.29-42		

1.2.	1 Чтение и анализ литературы:[3] с.229-231 2 Чтение и анализ литературы:[3] с.231-239 3 Чтение и анализ литературы:[3] с.231-239 4 Изучение конспекта лекций: [3]с.235-236 5 Изучение конспекта лекций: [3]с. 488-491 6 Чтение и анализ литературы:[3] с.239-241 7 Чтение и анализ литературы:[3] с.262-271, [9] с. 77-84 8 Чтение и анализ литературы:[3] с.271-282, [9] с. 84-88 9 Чтение и анализ литературы:[3] с.282-291 10 Чтение и анализ литературы:[9] с. 115-120, моделирование ситуаций		
1.3.	1 Чтение и анализ литературы:[3] с.40-42 2 Чтение и анализ литературы:[3] с.65-71 3 Чтение и анализ литературы:[3] с.293-307 4 Чтение и анализ литературы:[3] с.323-324 5 Чтение и анализ литературы:[3] с.324-333 6 Чтение и анализ литературы:[3] с.333-341 7 Чтение и анализ литературы:[3] с. 346-362 8 Чтение и анализ литературы:[3] с.380-416		
Тема 1.4 Защита серверных частей виртуальной защищенной сети	**Содержание**		**22**
	1	**Организация туннеля** Подготовка к установке ПО VipNet Координатор. Формирование VPN-сети. Настройка маршрутизации в локальных сетях Установка ПО VipNet Координатор. Первичная инициализация справочно-ключевой информации пользователя ПО VipNet Координатор. Развертывание VPN-сети и настройка СУ для совместной работы. Настройка туннелирования	4
	2	**Организация полутуннеля** Развертывание VPN-сети и настройка СУ для совместной работы. Настройка полутуннелирования	2
	3	**Режим работы сети«Открытый интернет»** Технология «Открытый интернет» Координатор Открытого интернета. VipNet клиенты Открытого Интернета.	2
	4	**Защита Клиентских рабочих мест при построении VipNet сетей** Требования к аппаратным средствам и операционной среде. Первичная инициализация	4

		пользователей. Доступ к компьютеру защищенной сети через межсетевой экран. Структура каталога. Режимы безопасности. Мониторинг активности приложений	
	5	**Доступ к туннелированным компьютерам** Монитор и деловая Почта. Работа с сертификатами ЭП пользователя Шифрование.	2
	6	**Администрирование сетевых узлов** Монитор и Администратор СУ. Криптопровайдер. Виды фильтров. Журналирование IP-пакетов. Транспортный модуль MFTP.Конвертор MFTP	2
	7	**Запуск внешних программ в ДП** ПО не входящее в состав защищенной сети. Запуск внешних программ	2
	8	**Технология автопроцессинга** Автоматизация серверной части для работы с входной и исходящей корреспонденцией. Правила безопасности.	2
	9	**Архивация. Автоархивация. Резервное копирование** Параметры архивации. Автоматическая архивация. Резервное копирование	2
	Практические занятия		**22**
	1-2	Настройка туннеля	4
	3-4	Настройка полутуннеля	4
	5-6	Настройка «Открытого интернета»	4
	7-8	Настройка сервера VipNet	4
	9 - 10	Настройка клиента VipNet	4
	11	Настройка резервного копирования	2
Тема 1.5 Технологии обнаружения и предотвращения вторжений	**Содержание**		**24**
	1	**Технология обнаружения атак** Концепция адаптивного управления безопасностью. Технология анализа защищенности.	2
	2	**Средства анализа защищенности сетевых протоколов и сервисов** Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности	2

	3	**Средства обнаружения сетевых атак** Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак	4
	4	**Система обнаружения вторжений (IDS)** Обнаружение вторжения. Прогноз возможных будущих атак. Сетевое зондирование (сканирование) или другое тестирование для обнаружения уязвимостей целевой системы. Выполнение документирования существующих угроз;	2
	5	**Архитектура IDS** Сенсорная подсистема, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы; Подсистема анализа, предназначенную для выявления сетевых атак и подозрительных действий; Хранилище, в котором накапливаются первичные события и результаты анализа; Консоль управления, позволяющая конфигурировать IDS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты.	2
	6	**Система предотвращения вторжений (IPS)** Программные и аппаратные решения. Мониторинг сети. Компьютерные системы в реальном времени.	2
	7	**Технологии защиты от вирусов** Компьютерные вирусы и проблемы антивирусной защиты цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ	2
	8	**Способы проникновения в систему** Классификация. Типы объектов. Вредоносные программы. Вирусы и черви Троянские программы. Подозрительные упаковщики. Вредоносные утилиты	2
	9	**Программы поведений** Adware, Pornware, Riskware.	2
	10	**Правила поглощения типов. Правила именования** Malware	2
	11	**Новые технологии** Проактивные технологии	2
	Практические занятия		**24**
	1	Kaspersky Internet Security	2
	2	Kaspersky Total Security	2

	3	Kaspersky Endpoint Security	2
	4	Kaspersky Endpoint Security CLOUD	2
	5-6	Kaspersky Anti Targeted Attack Platform	4
	7-8	Kaspersky Защита для центров обработки данных	4
	9-10	Защита от DDoS-атак	4
	11 12	Защита критических инфраструктур	4
Тема 1.6 Методы управления средствами защиты	**Содержание**		**6**
	1	**Методы управления средствами сетевой защиты** Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты	2
	2	**Аудит безопасности информационной системы.** Мониторинг безопасности системы. Программные средства проведения аудита безопасности.	2
	3	**Обзор современных систем управления сетевой защитой** Классификация систем защиты. Перспективы и тенденции в развитии систем защиты	2
	Практические занятия		**6**
	1	Nmap	2
	2	X-Spider	2
	3	Max-Patrol	2
Самостоятельная работа при изучении раздела ПМ.2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя. Оформление практических работ, отчетов и подготовка к их защите.			**6**
Примерная тематика домашних заданий			
1.4	1 Чтение и анализ литературы [3] с.171-189 2 Чтение и анализ литературы [3] с.189-191 3 Чтение и анализ литературы [3] с.191-197 4Чтение и анализ литературы [3] с.199-211 5 Чтение и анализ литературы [3] с.2-11-221 6 Чтение и анализ литературы [3] с.222-234		

	7 Чтение и анализ литературы [3] с.236-243 8 Чтение и анализ литературы [3] с.243-252 9 Чтение и анализ литературы [3] с.252-277	
1.5	1 Чтение и анализ литературы:[3] с.427-435 2 Чтение и анализ литературы:[3] с.436-439 3 Чтение и анализ литературы:[3] с.439-453 4 Чтение и анализ литературы:[3] с.453-464, 464-481 5 Чтение и анализ литературы [3] с.481-492 6 Чтение и анализ литературы [3] с.492-495 7 Чтение и анализ литературы [3] с.496-497 81 Чтение и анализ литературы [3] с.498-502 9 Чтение и анализ литературы [3] с.502-505 10 Чтение и анализ литературы [3] с.505-511 11 Чтение и анализ литературы [3] с.511-512	
1.6	1 Чтение и анализ литературы:[3] с.481-496 2 Чтение и анализ литературы:[3] с.496-501 3 Чтение и анализ литературы:[3] с.501-507	
Курсовая работа(проект)		**20**
Промежуточная аттестация (экзамен)		**12**

IV семестр

Раздел 2. Методы криптографической защиты информации			
МДК 2.2 Криптографическая защита информации			
Тема 2.1 Основы криптографических методов защиты информации	**Содержание**		**20**
	1	**Свойства информационной безопасности** Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности	2

.	2	**Криптографические методы** Шифрование. Кодирование. Стеганография. Сжатие	2
	3	**Математика криптографии** Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение	2
	4	**Традиционные шифры перестановки** Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования	2
	5	**Традиционные шифры замены** Шифры замены. Шифры многоалфавитной замены. Частотность символов.	2
	6	**Криптоанализ шифров перестановки** Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста	2
	7	**Криптоанализ шифров замены** Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста	2
	8	**Компьютерное шифрование** Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей	2
	9	**Современная компьютерная стеганография** Контейнеры. Скрытие информации в изображениях, текстовых файлах, видеозаписях.	2
	10	**Свойства информационной безопасности** Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности	2
	Практические занятия		**20**
	1	Бинарная арифметика. Модульная арифметика	
	2	Применение методов шифрования перестановкой	
	3	Применение методов шифрования заменой	
	4	Применение методов шифрования многоалфавитной замены	
	5-6	Криптоанализ методов перестановки	
	7-8	Криптоанализ методов замены	
	9	Компьютерное шифрование	
	10	Стеганографические методы скрытия информации	
Тема 2.2 **Современные стандарты шифрования**	**Содержание**		**14**
	1	**Симметричное шифрование** Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное	2

		применение DES. Безопасность DES	
	2	**Усовершенствованный стандарт шифрования AES** Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES	2
	3	**Российские стандарты симметричного шифрования** Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015	2
	4	**Проблема распределения ключей симметричного шифрования** Алгоритм Диффи-Хелмана. Управление ключами.	2
	5	**Асимметричное шифрование RSA** Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках.	2
	6	**Асимметричное шифрование на основе логарифмов** Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов	2
	7	**Криптосистемы на основе метода эллиптических кривых.** ЭЦП. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов ГОСТ Р 34.12-2015	2
	Практические занятия		**14**
	1	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	2
	2	Ассиметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	2
	3	RSA	2
	4	Криптосистема Эль-Гамаля	2
	5	AES	2
	6	ГОСТ 28147-89	2
	7	ГОСТ Р 34.12-2015	2
Тема 2.3 Криптографические методы обеспечения безопасности сетевых технологий	**Содержание**		**16**
	1	**Целостность сообщения** Случайная модель Orac1e. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции	2
	2	**Электронная цифровая подпись** Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП. ГОСТ Р	2

		34.10 -2012.	
	3	**Установление подлинности объекта** Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены	2
	4	**Проблемы распределения открытого ключа асимметричного шифрования** Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI	2
	5	**Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне** Электронная почта. Архитектура e-mail. PGP. S/M1ME	2
	6	**Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне** Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети	2
	7	**Защита информации в сетях организованных по технологии беспроводного доступа** IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16	2
	8	**Защита информации в сетях сотовой связи** A3. A8.A5/3. Атаки на алгоритмы Перспективы развития беспроводной мобильной связи	2
	Практические занятия		**16**
	1	Обеспечение целостности. Алгоритм MD5	2
	2	Обеспечение целостности. Алгоритм SHA	2
	3	Электронная подпись RSA	2
	4	Электронная подпись ГОСТ34.10-2012	2
	5	Пароль. Проверка надежности.	2
	6	Динамический пароль	2
	7, 8	OpenSSL	4
Самостоятельная работа при изучении раздела ПМ 2. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя. Оформление практических работ, отчетов и подготовка к их защите.			
Примерная тематика домашних заданий			

2.1.	1.Чтение и анализ литературы: [1] с.19-28 2.Чтение и анализ литературы: [1] с.28-32 3.Чтение и анализ литературы: [1] с.37-66 4.Чтение и анализ литературы: [1] с.73-111 5.Чтение и анализ литературы: [1] с.73-111 6.Чтение и анализ литературы: [1] с.73-111 7. Чтение и анализ литературы: [1] с. 119-130, изучение конспекта лекций 8. Чтение и анализ литературы: [1] с.73-111 9. Чтение и анализ литературы: [1] с.73-111 10. Чтение и анализ литературы: [1] с.73-111	
2.2.	1.Чтение и анализ литературы: [1] с.183-211, [3] с.117-121 2.Чтение и анализ литературы: [1] с.215-244, [3] с.128-131 3. Чтение и анализ литературы: [3] с.124-128, изучение конспекта лекций 4.Чтение и анализ литературы: [1] с.471-487, решение вариативных задач 5.Чтение и анализ литературы: [1] с.318-359, [3] с. 156-161, решение вариативных задач 6. Чтение и анализ литературы: [1] с.318-359, [3] с. 156-161, решение вариативных задач 7. Чтение и анализ литературы: [1] с.318-359, [3] с. 156-161, решение вариативных задач	
2.3.	1.Чтение и анализ литературы: [1] с.366-386, решение вариативных задач 2.Чтение и анализ литературы: [1] с.419-441, решение вариативных задач 3.Чтение и анализ литературы: [1] с.448-468, решение вариативных задач 4.Чтение и анализ литературы: [1] с.487-497 5.Чтение и анализ литературы: [1] с.501-539 6.Чтение и анализ литературы: [1] с.542-601, [3] с.334-378 7.Чтение и анализ литературы: [2] с.235-256, [3] с. 341-345 8.Чтение и анализ литературы: [2] с.186-201	

V семестр

Тема 2.4 Средства и услуги в области криптографической защиты информации,	**Содержание**		**26**
	1	**Средства криптографической защиты информации «КриптоПро»** Средства криптографической защиты информации. КриптоПро CSP. КриптоПро ЭП. КриптоПро JCP .КриптоПро .NET. КриптоПро IPSec. КриптоПро HSM. Атликс HSM. КриптоПро AirKey	2
	2	**Средства криптографической защиты информации со смарткартами и USB ключами**	2

представленные на отечественном рынке		КриптоПро CSP для универсальной электронной карты. Магистра CSP. КриптоПро Рутокен CSP. КриптоПро ФКН CSP 3.9. КриптоПро CSP 4.0 ФКН (Gemalto)	
	3	**Инфраструктура открытых ключей КриптоПро** Удостоверяющий центр КриптоПро УЦ. КриптоПро TSP. КриптоПро OCSP. КриптоПро SVS. АРМ разбора конфликтных ситуаций. КриптоПро Revocation Provider. КриптоПро ЭЦП. КриптоПро ЭЦП Browser plug-in. КриптоПро SSF КриптоПро DSS. КриптоПро DSS Lite	2
	4	**Защита от несанкционированного доступа с использованием КриптоПро CSP** КриптоПро TLS. КриптоПро Stunnel. КриптоПро Winlogon. КриптоПро EAP-TLS СЗИ Secure Pack Rus 3.0. КриптоПро EFS	2
	5	**Системы идентификации Программы и утилиты** IdM. КриптоАРМ (Крипто Три). Приложение командной строки cryptcp Браузер КриптоПро Fox. ЭЦП процессор. КриптоПро PDF. КриптоПро Office Signature. КриптоПро CRM	2
	6	**Клиентские компоненты средств информационной безопасности «Инфотекс»** ViPNet Client. ViPNet Personal Firewall. ViPNet Client Mobile ViPNet Connect. ViPNet CryptoFile. ViPNet CSP	2
	7	**Серверные компоненты средств информационной безопасности «Инфотекс»** ViPNet Coordinator HW. ViPNet Coordinator KB. ViPNet Coordinator Software. ViPNet HSM. ViPNet IDS. ViPNet Industrial Gateway	2
	8	**Компоненты управления «Инфотекс»** ViPNet Administrator. ViPNet Statewatcher. ViPNet Certification Authority. ViPNet Policy Manager	2
	9	**Криптографическая линейка продуктов компании «Аладдин»** JaCarta. "Антифрод-терминал". JC-WebClient. JaCarta SecurLogon. ПО JaCarta АРМ УЦ. "КриптоПро ФКН CSP"	2
	10	**Семейство Secret Disk** Secret Disk Enterprise. Secret Disk Server NG. Secret Disk 5. Сертификаты Алгоритмы шифрования. Защита 1С:Предприятие	2
	11	**НТЦ Атлас** «Атликс-VPN»,«Модуль-HSM». Однонаправленный шлюз «Атликс-Шлюз-К» Программно-аппаратный комплекс (ПАК) «Криптосервер». Система обнаружения сетевых атак программно-аппаратный комплекс "Тор". Комплексная система голографического и криптографического контроля целостности документов (КСГК)	2
	12	**Продукты Рутокен**	2

		Рутокен ЭЦП 2.0. Рутокен Lite. Рутокен S. Рутокен ЭЦП 2.0 Flash. Рутокен ЭЦП PKI. Рутокен PINPad. Рутокен ЭЦП Bluetooth. Рутокен Web. Рутокен VPN. Рутокен Плагин. Рутокен для Windows. КриптоТри. Рутокен KeyBox. КриптоПро Рутокен CSP	
	13	**Продукты Анкад** Средства для работы с ключевой информацией Crypton VPN Защищенный тонкий клиент КРИПТОН-ЗАМОК Комплекс аппаратно-программных средств ограничения доступа	2
	Практические задания		**26**
	1	Изучение и настройка СЗИ Рутокен ЭЦП 2.0.	2
	2	Изучение и настройка СЗИ Рутокен PINPad	2
	3	Изучение и настройка СЗИ Рутокен Web.	2
	4	Изучение и настройка СЗИ Рутокен ЭЦП Bluetooth	2
	5	Изучение и настройка СЗИ Secret Disk	2
	6	Изучение и настройка СЗИ КриптоПро CSP.	2
	7	Изучение и настройка СЗИ КриптоПро ЭП.	2
	8	Изучение и настройка СЗИ КриптоПро УЦ.	2
	9	Изучение и настройка СЗИ КриптоПро Stunnel.	2
	10	Изучение и настройка СЗИ ViPNet Client.	2
	11	Изучение и настройка СЗИ ViPNet Personal Firewall.	2
	12	Изучение и настройка СЗИ ViPNet Coordinator HW.	2
	13	Изучение и настройка СЗИ ViPNet Administrator.	2
Курсовая работа(проект)			**10**
Примерная тематика курсовых проектов			
1	Защита информации с применением СЗИ Рутокен ЭЦП Bluetooth		
2	Защита информации с применением СЗИ Secret Disk		
3	Защита информации с применением СЗИ КриптоПро CSP.		
4	Защита информации с применением СЗИ КриптоПро ЭП.		
5	Защита информации с применением СЗИ КриптоПро УЦ.		
6	Защита информации с применением СЗИ КриптоПро Stunnel.		
7	Защита информации с применением СЗИ ViPNet Client.		
8	Защита информации с применением СЗИ ViPNet Personal Firewall.		
9	Защита информации с применением СЗИ ViPNet Coordinator HW.		
10	Защита информации с применением с		

	СЗИ ViPNet Administrator.	
Промежуточная аттестация (экзамен)		**8**
Учебная практика 2.01 **Виды работ**		**108**
1	Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. Разработка маркетингового плана продвижения услуг связи. Выявление конкурентного преимущества на рынке. Проведение маркетингового исследования рынка услуг связи/ Анализ внешней микросреды маркетинга	6
2	Подключение, установка драйверов, настройка программных средств шифрования Криптон. Администрирование программных средств шифрования Криптон	6
3	Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. Администрирование аппаратных средств шифрования Криптон	6
4	Выбор, подключение, настройка межсетевого экрана. Администрирование межсетевого экрана.	6
5	Ознакомление, подключение, настройка системы резервного копирования Администрирование системы резервного копирования	6
6	Ознакомление, подключение, настройка системы антивирусной защиты. Администрирование системы антивирусной защиты	6
7	Изучение возможностей программы для контроля действий сотрудников, потоков информации и событий системы StaffCopEnterprise	6
8	Контроль электронной почты с помощью программы StaffCopEnterprise	6
9	Мониторинг файлов, отправляемых через интернет с сохранением их резервной копии с помощью программы StaffCopEnterprise	6
10	Анализ поисковых запросов с помощью программы StaffCopEnterprise	6
11	Мониторинг процессов и приложений с помощью программы StaffCopEnterprise	6
12	Ознакомление, подключение, настройка СЗИ Рутокен Web.	6
13	Изучение и настройка СЗИ Рутокен ЭЦП Bluetooth	6
14	Ознакомление, подключение, настройка СЗИ Secret Disk	6
15	Изучение и настройка СЗИ КриптоПро CSP.	6
16	Ознакомление, подключение, настройка СЗИ КриптоПро ЭП.	6
17	Изучение и настройка СЗИ КриптоПро УЦ.	6
18	Оформление отчета. Участие в зачет - конференции по учебной практике	6
Производственная практика (по профилю специальности) 2.02 **Виды работ**		**144**
1	Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике.	6
2	Подключение, установка драйверов, настройка программных средств абонентского шифрования	6

3	Администрирование внедренных средств	6
4	Настройка средств электронной подписи	6
5	Администрирование средств электронной подписи	6
6	Администрирование средств PKI	6
7	Участие в организации работ по защите персональных компьютеров на предприятии	6
8	Участие в организации работ по защите локальных сетей на предприятии	6
9	Участие в организации работ по защите работ в глобальной сети интернет на предприятии	6
10	Моделирования угроз, расчет рисков информационной безопасности	6
11	Администрирование проводной защищенной локальной сети .	6
12	Ознакомление, организация, настройка беспроводной защищенной локальной сети.	6
13	Подключение, установка драйверов, настройка программных средств СЗИ КриптоПро Stunnel.	6
14	Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Client.	6
15	Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Personal Firewall.	6
16	Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Coordinator HW.	6
17	Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Administrator.	6
18	Администрирование СЗИ Рутокен ЭЦП 2.0.	6
19	Изучение и настройка СЗИ Рутокен PINPad	6
20	Администрирование СЗИ Рутокен Web.	6
21	Изучение и настройка СЗИ Рутокен ЭЦП Bluetooth	6
22	Администрирование СЗИ Secret Disk	6
23	Изучение и настройка СЗИ КриптоПро CSP.	6
24	Оформление отчета. Участие в зачет- конференции по производственной практике	6
	Промежуточная аттестация (экзамен (квалификационный))	**6**
	Всего:	**715**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие лаборатории программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета и рабочих мест кабинета:
- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-методических документации;
- дидактические материалы.
- учебно-наглядные пособия по дисциплине «Информационная безопасность и защита информации»:
- плакаты:
  - «Модель информационной безопасности»;
  - «Технические каналы утечки информации»;
  - «Односторонне функции шифрования»;
  - «Модель угроз информационной безопасности»;
  - «Сертификаты открытых ключей»
- презентации:
  - «Технические средства защиты информации»;
  - «Инженерно технические средства защиты информации»;
  - «Средства криптографической защиты информации»;
- учебный фильм:«Зашифрованная война»
- мультимедиапроектор, компьютер преподавателя;

Оборудование лаборатории программно-аппаратных средств обеспечения информационной безопасности:
- технические средства обучения:
- персональные компьютеры (объединенные в учебную локально-вычислительную сеть с выходом в сеть Интернет) по количеству обучающихся с лицензионным программным обеспечением: ОС Windows XP, Windows Server 2003, ОС Unix;
- учебно-лабораторный комплекс «Криптон» (Платы «Криптон-замок», аппаратные абонентские и сетевые шифраторы, программное обеспечение);
- учебно – лабораторный комплекс беспроводной сети Wi-Fi;
-лабораторное измерительное оборудование:
  - осциллограф -2 шт.;
  - частотомер – 2 шт.;
  - генератор – 1 шт.;
  - мультиметр – 4 шт.;
  - источник питания – 6 шт.;
  - паяльная станция – 2 шт.;
  - демонтажная станция -1 шт.;
  - анализатор поля – 1 шт.;

- измеритель электромагнитного поля – 1 шт.;
- детектор излучений -1 шт.;
- индикатор СВЧ -1шт;
- тестер кабельных линий -1 шт.;

- лабораторные стенды:
- «Изучение системы видеонаблюдения»;
- «Изучение систем контроля доступа»;
-«Изучение беспроводной системы охранно-пожарной сигнализации»;
- «Светочувствительная сигнализация»
- «Микроконтроллерное устройство управления исполнительными блоками для режимных объектов»
- «Микропроцессорное автоматическое устройство управления системой принудительного охлаждения телекоммуникационной стойкой аппаратуры по 4 каналам измерения в реальном масштабе времени»
- «Изучение биометрических систем контроля доступа»
- «Структурированные кабельные системы NIKOMAX»

Реализация программы модуля предполагает обязательную учебную практику.
Оборудование и технологическое оснащение рабочих мест:
- рабочее место (ПК, монитор, мышь, клавиатура) (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i5, оперативная память объемом не менее 16 Гб; HD 10000 Gb,
- программа для контроля действий сотрудников, потоков информации и событий системы StaffCopEnterprise

3.2. Информационное обеспечение обучения

Основные источники:

1. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие/ Фороузан Б.А.; пер. с англ. Под ред.А.Н. Берлина. - М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2019.-784с.:ил.,табл.-(Основы информационных технологий).
2. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи/ Под ред. доктора техн. Наук, профессора О.Б. Макаревича. – М.: Горячая линия – Телеком, 2016. -360с.: ил.
3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства –М.: ДМК Пресс, 2019. – 544с.:ил.
4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2019.-272с.:ил.
5. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2016.-528с.-(Профессиональное образование)
6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для вузов -5-е изд., перераб. и доп. – М.: - Горячая линия – Телеком, 2016. – 616с:ил.

7.Романов О.А. Организационное обеспечение информационной безопасности: учебник для студентов высш. учеб. заведений –М.: Издательский центр «Академия», 2019. – 192с.
8. Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/. – М.: Издательский центр «Академия», 2017. – 336с
9. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябовд.Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2016. – 363 с.
10.Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов, 5-е изд. – Спб.: Питер, 2015. – 944 с.
11.Томаси У. Электронные системы связи. - М.: Техносфера, 2016. -1360с.
12.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2016. – 184 с.
13.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2016. – 172 с.
14.Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с
15.В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2018
16.Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2018. – 416 с.
17.Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2018. - 192с.

Дополнительные источники:

1 Руководство администратора Криптон-замок
2. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. Пособие для студ. Высш. Учеб. Заведений – М.: Издательский дом «Академия», 2016. – 240с.
3. Торокин А.А. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в обл. информ. Безопасности – М.:Гелиос АРВ, 2015 – 960с.: ил. – ISBN 5-85438-140-0.
4. Руководство администратора ППКОП «Астра»
5. Руководство администратора КТМ-256
6. Учебное пособие Структурированная кабельная система NIKOMAX»

Интернет ресурсы:

1. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http:// www.znanium.com/ (2019).
2. http://www.fstec.ru сайт ФСТЭК РФ
3. http://www.ancad.ru сайт компании АНКАД
4. https://www.cryptopro.ru/ сайт компании КриптоПро
5. https://infotecs.ru/ сайт ОАО «ИнфоТеКС»

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ПО РАЗДЕЛАМ)

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

ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен