Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

КОЛЛЕДЖ КОСМИЧЕСКОГО МАШИНОСТРОЕНИЯ И ТЕХНОЛОГИЙ

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

10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

Королев, 2023 г.

Авторы: Родичкин П.Ф., Чебышев А.Ю. 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». – Королев МО: ТУ им. А.А. Леонова, 2023 г.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования (далее - ФГОС СПО) и Учебного плана по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа рассмотрена и одобрена на заседании цикловой комиссии по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем 16 мая 2023 г., протокол № 6.

Рабочая программа учебной дисциплины рекомендована к реализации в учебном процессе на заседании учебно-методического совета 17 мая 2023 г., протокол № 5.

Содержание

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Место модуля в структуре образовательной программы

Профессиональный модуль «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты» принадлежит к профессиональному циклу.

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид и соответствующие ему профессиональные компетенции:

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное решение.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.
ЛР 09	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 13	Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности
ЛР 14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
ЛР 22	Способный проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных
ЛР 23	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.
ЛР 24	Принимающий правила внутреннего распорядка обучающихся в части выполнения обязанностей

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 несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических, средств защиты информации.

1.2.3. В результате освоения профессионального модуля обучающийся должен:

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

1.3. Количество часов, отводимое на освоение профессионального модуля:

Всего часов 588

Из них на освоение МДК 384 часа

в том числе самостоятельная работа 16 часов

практики, в том числе учебная 108 часов

производственная 72 часа

Промежуточная аттестация 24 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Тематический план профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля		Объем профессионального модуля, ак. час.							
		Суммарный объем нагрузки, час.	Работа обучающихся во взаимодействии с преподавателем							Самостоятельная работа
			Обучение по МДК				Практики		Консультации	
			Всего	В том числе			Учебная	Производственная		
				Промежут. аттест.	Лаборат. и практ. занятий	Курсовых работ (проектов)				
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ПК 2.1 – ПК 2.3 ОК 01- ОК 04, ОК 09, ОК 10	Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	**240**	**232**	**-**	**66**	**20**	**-**	**-**	**-**	**8**
ПК 2.1 – ПК 2.3 ОК 01- ОК 04, ОК 09, ОК 10	Раздел 2. Криптографическая защита информации	**144**	**136**		**54**	**-**	**-**	**-**	**-**	**8**
Учебная практика		**108**					**108**			
Производственная практика (по профилю специальности), часов		**72**						**72**		
Промежуточная аттестация (экзамен квалификационный)		**24**	**24**							
	Всего:	**588**	**384**		**120**	**20**	**108**	**72**	**-**	**16**

2.2. Содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов
1	2	3
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**240**
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		232
Тема 1. Обеспечение безопасности операционных систем	**Содержание**	**26**
	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows 10, Windows 7, Windows8. Linux. QNX и другие операционные системы. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации Пароли. PIN-коды. Методы надежного составления паролей. Строгая аутентификация. Односторонняя аутентификация. Двухсторонняя аутентификация Аппаратно-программные средства идентификации и аутентификации. Токены. Смарт-карты. Виртуальные ключи. Программно-аппаратные модули доверенной загрузки. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. АПМДЗ Криптон - Замок системный администратор. Изучение настроек системного администратора АПМДЗ. АПМДЗ Криптон - Замок, настройки пользователя АПМДЗ. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ Сектор НЖМД. Область памяти. Файл, папка, каталог.	
	Практические и лабораторные работы	**10**

	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав пользователя Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудитаНастройка изолированной среды АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование Восстановление информации типовыми средствами Программы восстановление информации	
Тема 2. Технологии разграничения доступа	**Содержание**	**26**
	Архитектура подсистемы защиты операционной системы Windows Server2016. Особенности ОС Windows Scrver2016. Возможности администратора. Разграничение доступа к объектам операционной системы. Модели доступа. Дискреционная модель. Мандатная модель. Роли. Локальная политика безопасности. Настройка локальной политики безопасности. Администрирование системы. Изолированная программная среда. Способы организации. Методы применения. ActiveDirectory. Комплексная система организации управления доступом. Инсталяция. Настройка. Аудит безопасности операционной системы. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможно¬сти МЭ. Особенности функционирования межсетевых экранов. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Схемы защиты на базе межсетевых экранов. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.	
	Практические и лабораторные работы	**10**

	Программы надежного удаления информации Архивирование информации Программные средства резервного копирования. Настройка RAID-массивов Инсайдерская информация. Программы сбора информации о ПК Настройка межсетевого экрана.	
Тема 3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание**	**26**
	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/1P.Обеспсчение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. VPN - решения для построения защищенных сетей. Виртуальные защищенные сети. Туннелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом. Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	
	Практические и лабораторные работы	**14**
	Основные действия с виртуальной машиной Работа с контрольными точками Использование внешних устройств Работа с локальным хранилищем сертификатов в ОС WINDOWS Установка и настройка ПО eTokenPKIClient Настройка ПО eTokenPKIClient с помощью групповых политик Развертывание TMS в среде Active Directory	

	Настройка TMS вереде Active Directory Настрой капо литик TMS Настройка использования виртуального токена Использование токена на рабочем месте администратора Установка и настройка СКЗИ «КриптоПроСЗР» Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP Применение SecretDisk4 Применение SecretDisk Server NG Изучение основных возможностей ПО VipNetClient Изучение настроскПО VipNetClient Изучение возможностей ПО Деловая почта	
Тема 4. Технологии обнаружения вторжений	**Содержание**	**26**
	Технология обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак. Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.	
	Практические и лабораторные работы	**6**
	Изучение средств обнаружения атак Изучение антивирусных продуктов	
Тема 5. Методы	**Содержание**	**14**

управления средствами защиты	Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. Обзор современных систем управления сетевой защитой. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.	
Тема 6. Развертывание и эксплуатация DLP-систем	**Содержание**	**36**
	Оснастка групповых политик домена gpmc.msc. Интерактивный вход в систему в домене Active Directory Оснастка локальных групповых политик gpedit.msc Развёрывание программного обеспечения с помощью доменных групповых политик DHCP – настройки области аренды IP-адресов Брандмауэр Windows Server 2019, режим повышенной безопасности. Открытие и закрытие портов TCP и UDP. Настройка программного обеспечения для работы в сети Общий подход к защите конфиденциальных данных. Разграничение сетевых ресурсов. Подразделение в Active Directory (Organization Unit), группы пользователей. Объекты групповых политик Подключение компьютеров к домену, доменные учетные записи группы Администраторы Настройка сетевого взаимодействия, общие папки, назначение прав доступа Установка DLP-системы. Подготовка. Пользователь домена от имени которого будет установлена DLP-система. Выбор СУБД. Установка DLP-системы. Подготовка и установка СУБД DLP-система – развёртывание, настройка и администрирование Серверы DLP-системы. Центральный сервер, консоль администратора Серверы DLP-системы. Сервер контроля агентов, сервер расследований и другие Пользователи в DLP-системе. Интеграция с Active Directory Мониторинг состояния DLP-системы. Запуск и остановка серверов. Действия при возникновении ошибок Настройка центрального сервера DLP-системы. Хранение информации. Авторизация серверов. Настройка центрального сервера DLP-системы. Лицензирование. Настройка поисковых словарей. Настройка центрального сервера DLP-системы. Настройка цифровых отпечатков, настройка банков хешей Работа с пользователями и привилегиями. Синхронизация с Active Directory. Журнал авторизации. Установка и настройка агентов. Настройка сервера агентов. Хранилище записей аудио-видео мониторинга. Управление агентами, отслеживание состояния DLP-система - эксплуатация Мониторинг сетевой активности пользователей, настройки уровня рисков возникновения инцидентов Управление модулем Политики безопасности. Контроль активности пользователей. Аудио и видео	

	мониторинг. Мониторинг файловых систем. Политики безопасности. Просмотр уведомлений и системных событий. Экспорт и импорт данных. Расследования: настройки модуля. Создание и ведение дел Работа с модулем Отчеты	
	Практические и лабораторные работы	**26**
	Установка DLP-системы. Подготовка и установка СУБД DLP-система – развёртывание, настройка и администрирование Мониторинг состояния DLP-системы. Настройка центрального сервера DLP-системы. Хранение информации. Авторизация серверов. Лицензирование. Настройка поисковых словарей. Настройка цифровых отпечатков, настройка банков хешей. Работа с пользователями и привилегиями. Синхронизация с Active Directory. Журнал авторизации. Установка и настройка агентов. Настройка сервера агентов. Управление агентами, отслеживание состояния DLP-система – эксплуатация Мониторинг сетевой активности пользователей, настройки уровня рисков возникновения инцидентов Управление модулем Политики безопасности. Контроль активности пользователей. Аудио и видео мониторинг. Мониторинг файловых систем. Просмотр уведомлений и системных событий. Экспорт и импорт данных. Расследования: настройки модуля. Создание и ведение дел. Работа с модулем Отчеты	
Самостоятельная учебная работа при изучении раздела 1 ПМ		**8**
Учебная практика по профессиональному модулю **Виды работ:** Выбор, подключение, настройка межсетевого экрана. Администрирование межсетевого экрана. Ознакомление, подключение, настройка системы резервного копирования Администрирование системы резервного копирования. Ознакомление, подключение, настройка системы антивирусной защиты. Администрирование системы антивирусной защиты. Развертывание и эксплуатация DLP-системы Развертывание системы сертификации Работа с ПО для выпуска сертификатов безопасности		**108**
Тематика курсовых проектов: Проблемы обеспечения безопасности операционных систем. Аутентификация, авторизация и администрирование действий пользователя. Программно-аппаратные модули доверенной загрузки. Разграничение доступа к объектам операционной системы.		**20**

Комплексная система организации управления доступом. Аудит безопасности операционной системы. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Политика межсетевого взаимодействия. Классы МЭ. Требования ФСТЭК к МЭ. Концепция построения виртуальных защищенных сетей. Виртуальные защищенные сети. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Протоколы PAP, CHAP,S/Key, SSO, Kerberos. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы.		
Раздел 2. Криптографическая защита информации		**144**
МДК.02.02. Криптографическая защита информации		**136**
Тема 1.1. Основы криптографических методов защиты информации	**Содержание**	**26**
	Свойства информационной безопасности. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности. Криптографические методы. Шифрование. Кодирование. Стеганография. Сжатие. Математика криптографии. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Традиционные шифры перестановки. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. Традиционные шифры замены. Шифры замены. Шифры многоалфавитной замены. Частотность символов. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста . Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	
	Практические и лабораторные работы	**10**
	Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Действия с матрицами, бинарные операции, сравнение по модулю	

	Традиционные шифры перестановки Шифры перестановки. Поточные и блочные шифры. Механизация шифрования. Шифрование методами перестановки. Шифрование методом замены (подстановки). Шифрование методами перестановки. Шифрование методом замены (подстановки) Криптоанализ зашифрованного текста Шифрование и кодирование исходного текста. Расшифрование криптограммы и декодирование текста.	
Тема 1.2. Современные стандарты шифрования	**Содержание**	**28**
	Симметричное шифрование Сеть Фейстеля Стандарт шифрования данных DES. Структура DES. Применение DES. Безопасность DES Усовершенствованный стандарт шифрования AES Структура AES. Расширение ключей AES 128/192/256. Российский стандарт симметричного шифрования ГОСТ 28147-89 Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89 Проблема распределения ключей симметричного шифрования Алгоритм Диффи-Хеллмана. Управление ключами. Протокол сетевой аутентификации Kerberos. Асимметричное шифрование Простые числа и уравнения. Разложение на множители. Теорема об остатках. Возведение в степень и логарифмы. Криптографический алгоритм с открытым ключом RSA. Безопасность асимметричных алгоритмов Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. Целостность сообщения Случайная модель Oracle. Установление подлинности сообщения Криптографические хэш-функции. MD-5. SHA-1. SHA-512. Криптографические хэш-функция ГОСТ Р 34.11-94 Атаки на хэш-функции Установление подлинности объекта Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. Электронная цифровая подпись Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП Схемы цифровой подписи. ЭЦП с временной меткой. Атаки на цифровую подпись. Слепая подпись. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10-2012 Проблемы распределения открытого ключа асимметричного шифрования Сертификаты открытого ключа. Удостоверяющие центры. Формат сертификата X.509	
	Практические и лабораторные работы	**24**
	Симметричное шифрование, сеть Фейстеля Анализ симметричного шифрования DES. Анализ безопасности AES. Анализ шифрования ГОСТ 28147-89 Анализ алгоритма обмена ключами в протоколе Диффи-Хеллмана.	

	Анализ протокола сетевой аутентификации Kerberos. Анализ шифра RSA Шифрование Шифрование с помощью криптосистемы Эль-Гамаля. Анализ хэш-функции MD-5 Анализ ГОСТ 34.10-94. Средства криптозащиты идентификации и аутентификации Биометрические средства идентификации. Электронные ключи и карты. Алгоритм формирования электронной подписи Анализ ГОСТ Р 34.10-2012 Анализ дополнений сертификата X.509	
Тема 1.3. Криптографические методы обеспечения безопасности сетевых технологий	**Содержание**	**16**
	Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне Электронная почта. Архитектура e-mail. S/MIME. PGP. Обеспечение безопасности сети с применением криптографических протоколов на транспортном уровне Безопасность транспортного уровня. Форматы криптографических алгоритмов, применяемых в протоколах SSL. TLS. Обеспечение безопасности сети с применением криптографических протоколов на сетевом уровне IPSec. Транспортный режим. Режим туннелирования. Организация VPN-сети Криптовалюты Биткоин. Блокчейн. Технология Ethereum. Защита информации в сетях организованных по технологии беспроводного доступа IEEE 802.11. IEEE 802.16 WEP. WPA. WPA-2. Защита информации в сетях сотовой связи A3 A8 A5/3. Перспективы развития беспроводной мобильной связи Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования.	
	Практические и лабораторные работы	**10**
	Анализ протокола PGP Анализ протокола SSL. Анализ протокола TLS Анализ протокола IPSec. Анализ средств криптозащиты VPN-сетей Анализ средств криптозащиты криптовалюты Анализ средств криптозащиты технологии беспроводного доступа Анализ алгоритма шифрования A5	
Самостоятельная учебная работа при изучении раздела модуля 2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)		**8**

Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	
Производственная практика профессионального модуля **Виды работ** 1. Участие в организации работ по защите персональных компьютеров на предприятии 2. Участие в организации работ по защите локальных сетей на предприятии 3. Участие в организации работ по защите работ в глобальной сети интернет на предприятии 4. Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. 5. Администрирование систем безопасности проводной защищенной локальной сети. 6. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. 7. Администрирование систем безопасности беспроводной защищенной локальной сети. 8. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. 9. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей 10. Подключение, установка драйверов, настройка программных средств абонентского шифрования 11. Администрирование внедренных средств 12. Настройка средств электронной подписи 13. Администрирование средств электронной подписи 14. Администрирование средств PKI	**72**
Тематика курсовых проектов: 1. Изучение новых технологий хранения информации. 2. Обзор современных программных и программно-аппаратных средств защиты. 3. Сравнительный анализ современных программных и программно-аппаратных средств защиты. 4. Криптографические методы.Шифрование. Кодирование. Стеганография. Сжатие. 5. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. 6. Традиционные шифры замены. Шифры многоалфавитной замены. Частотность символов. 7. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. 8. Компьютерное шифрование. 9. Стандарт шифрования данных DES. Структура DES. Безопасность DES. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. 10. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos.	10

11. Асимметричное шифрование. Криптографическая система Эль-Гамаля. ГОСТ 34.10-94. ГОСТ Р 34.10-2012. 12. Комплексная модель защиты информации на предприятии. 13. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 14. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 15. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 16. Проблема защиты информации в облачных хранилищах данных и ЦОДах 17. Защита сред виртуализации.	
Промежуточная аттестация (экзамен квалификационный)	**24**
Всего по профессиональному модулю	**588**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация профессионального модуля требует наличия учебной мастерской «Анализ защищенности информационных систем от внешних угроз».

Оборудование мастерской:

- рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- учебные наглядные пособия (таблицы, плакаты);
- тематические папки дидактических материалов;
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся.

Технические средства обучения:

- персональный компьютер с лицензионным программным обеспечением;
- мультимедиа проектор (проектор, экран);
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения.

Оборудование мастерской:

№	Наименование оборудования	Кол-во
1	Автоматизированное рабочее место: Системный блок: - Intel Core i7-9700; - базовая тактовая частота 3.0 ГГц; - количество физических ядер 8; - количество потоков 8; ОЗУ: - 16 Гб; ПЗУ: - SSD объемом 500 Гб, HDD объемом 1000 Гб; сетевой адаптер: - технология Ethernet стандарта 1000BASE-T. Монитор: - ЖКД Dell p2419h с диагональю 24" (2 шт.) Клавиатура Logitech без клавиши Power, подключение по USB Компьютерная мышь: Logitech, подключение по USB	20
2	Экран с проектором Panasonic PT-VW360	1

3	Телекоммуникационный шкаф 42U	2
4	Автоматизированное рабочее место: Системный блок: - Intel Core i7-9700; - базовая тактовая частота 3.0 ГГц; - количество физических ядер 8; - количество потоков 8; ОЗУ: - 16 Гб; ПЗУ: - SSD объемом 500 Гб, HDD объемом 1000 Гб; сетевой адаптер: - технология Ethernet стандарта 1000BASE-T. Монитор: - ЖКД Dell p2419h с диагональю 24" (2 шт.)	4
5	Маршрутизатор Cisco ISR 4300 Series	10
6	Коммутатор Cisco 2960 plus	20
7	Межсетевой экран ASA 5506-X	10
8	Платформа RouterBoard MikroTik (Маршрутизатор, коммутатор, PoE)	20
9	Комплексный стенд по защите информации	1

Перечень программных средств:

№	Наименование	Количество лицензий
1	MS Windows 10	20
2	MS Office 2013 Pro Plus	20
3	Adobe reader	20
4	7-zip	20
5	Libre Office	20
6	Notepad++	20
7	Sublime Text 3	20
8	Visual Studio 2019	20
9	Visual Studio Code	20
10	WebStorm	20
11	VirtualBox	20
12	Putty	20
13	OpenServer (Ultimate)	20
14	Linux Debian / Linux Centos	20
15	Cisco Packet Tracer	20
16	Autodesk DWG TrueView	20
17	MS SQL Server Express	20
18	SQL Server Management Studio	20
19	MySQL Community Edition	20

3.2. Информационное обеспечение обучения

Основные источники:

1. Компьютерные сети. Принципы, технологии, протоколы Олифер Н.А, Олифер В.Г. // Учебник для вузов, 6-е изд. — Спб.: Питер, 2020. — 1019с.
2. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи Новикова Е. Л. Издательство Академия, 2018. - 190 с
3. Криптографическая защита информации в объектах информационной инфраструктуры. Учебник Ильин М.Е., Калинкина Т.И., Пржегорлинский В.Н. Издательство Академия, 2020. - 288 с.
4. Пакеты прикладных программ: Учебное пособие http://znanium.com/catalog.php?bookinfo=546662
5. Документация по Oracle VirtualBox: https://www.virtualbox.org/ wiki/Documentation
6. Документация производителя DLP-системы (Falcongaze, Infowatch)
7. Пакеты прикладных программ: Учебное пособие http://znanium.com/catalog.php?bookinfo=546662
8. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2021. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-557-8. https://znanium.com/catalog/document?id=364477
9. Учебное пособие https://mark.unitech-mo.ru/MarcWeb2/Found.asp
10. Крамаров С.О., Тищенко Е.Н., Соколов С.В., Шевчук П.С., Митясова О.Ю. Криптографическая защита информации: учеб. пособие для вузов / Издательство: РИОР, 2021-324 с.: -ISBN 978-5-16-106001-8 https://znanium.com/catalog/document?id=361143
11. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2021. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-557-8. https://znanium.com/catalog/document?id=364477
12. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2021. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6, 500 экз. https://znanium.com/read?id=367588

Дополнительные источники:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации».

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ (редакция, действующая с 1 марта 2021 года) «О персональных данных».

– Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (с изменениями на 9 марта 2021 года)

– Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (с изменениями на 9 марта 2021 года)

– Доктрина информационной безопасности Российской Федерации

– Положение «О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам» (извлечения). Утверждено Постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 № 912-51.

– Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О Стратегии национальной безопасности Российской Федерации»

– Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

– Указ Президента Российской Федерации от 22 декабря 2017 года № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

– Федеральный закон от 27 декабря 2002 г. № 184-ФЗ (с изменениями на 22 декабря 2020 года) «О техническом регулировании».

– Федеральный закон от 4 мая 2011 г. № 99-ФЗ (с изменениями на 31 июля 2020 года) «О лицензировании отдельных видов деятельности».

– Федеральный закон от 30.12. 2001 № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (с изменениями на 9 марта 2021 года) (редакция, действующая с 27 марта 2021 года).

– Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями на 31 августа 2020 года).

– Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями на 13 июля 2015 года).

– Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

– Положение о сертификации средств защиты информации. Постановление Правительства Российской Федерации от 26.06.1995 № 608.

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

– Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

– Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

– Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

– Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

– Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

Электронные издания (электронные ресурсы):

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
- Федеральный портал «Информационно - коммуникационные технологии в образовании» http://oso.rcsz.ru/info/kompas/edu.htm
- Всероссийский образовательный портал https://edu-ikt.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Таблица 1

Результаты освоения профессиональных компетенций

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и 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	Фронтальный и письменный опрос. Тестирование. 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.	Фронтальный и письменный опрос. Тестирование. 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	Фронтальный и письменный опрос. Тестирование. Экспертное наблюдение.

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
	(в том числе криптографических) средств защиты информации.	

Таблица 2

Результаты освоения общих компетенций

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
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;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 02 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.	Оценка деятельности обучающегося в процессе освоения образовательной программы на практических занятиях
ОК 03 Планировать и реализовывать собственное профессиональное и личностное решение.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы.	Оценка по результатам наблюдения за поведением в процессе освоения профессионального модуля и выполнения работ на практических занятиях, учебной практике, экзамене
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).	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 09 Использовать информационные технологии в профессиональной деятельности	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту.	Оценка по результатам наблюдения за поведением в процессе освоения профессионального модуля и выполнения работ на практических занятиях, учебной практике, экзамене (квалификационном)
ОК 10. Пользоваться профессиональной документацией на	эффективность использования в профессиональной деятельности необходимой	Оценка по результатам наблюдения за поведением в процессе освоения

государственном и иностранном языке.	технической документации, в том числе на английском языке.	профессионального модуля и выполнения работ на практических занятиях, учебной практике, экзамене (квалификационном)

Критерии оценки ответов

При оценке ответов дополнительно должны быть учтены качество сообщения, отражающего основные моменты и ответы на вопросы, заданные по теме вопроса.

Результаты защиты определяются оценками *«отлично», «хорошо», «удовлетворительно», «неудовлетворительно».*

1. Оценки ***«отлично»*** заслуживает ответ, в котором полно и всесторонне раскрыто теоретическое содержание темы, дан глубокий критический анализ действующей практики учетно-аналитической работы. Обучающийся при ответе дал аргументированные ответы на все вопросы преподавателя, проявил творческие способности в понимании и изложении ответов на вопросы.

2. Оценка ***«хорошо»*** выставляется за ответ, который имеет убедительный ответ. При его этом обучающийся показывает знания вопросов темы, оперирует данными, вносит предложения по теме ответа, во время ответа использует наглядные пособия, без особых затруднений отвечает на поставленные вопросы.

3. Оценка ***«удовлетворительно»*** выставляется за ответ, в котором имеются замечания по содержанию ответа и методике анализа. В теоретических, выводы в основном правильные, предложения представляют интерес, но недостаточно убедительно аргументированы и не на все вопросы обучающийся дал правильные ответы.

4. Оценка ***«неудовлетворительно»*** выставляется за ответ, который в основном отвечает предъявляемым вопросам, но обучающийся не дал правильных ответов на большинство заданных вопросов, т.е. обнаружил серьезные пробелы в профессиональных знаниях.