Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Амурский государственный университет»

УТВЕРЖДАЮ
Проректор по УиНР
_____ А.В. Лейфа
«__» ____ 2021 год.

РАБОЧАЯ ПРОГРАММА
по профессиональному модулю

ПМ.02. Защита информации в информационно - телекоммуникационных системах и сетях с использованием программных и программно- аппаратных (в том числе, криптографических) средств защиты

Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Квалификация выпускника – техник по защите информации
Год набора 2021
Курс 2,3 Семестр 3,4,5,6
Общая трудоемкость дисциплины 980 (час.)

Составитель: Батурин Д.С.

2021г.

Рабочая программа профессионального модуля разработана в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденный приказом Минобрнауки РФ от 09.12.2016 г. № 1551

Рабочая программа обсуждена на заседании ЦМК социально-экономических дисциплин
«25» 05 20 21 г., протокол № 6
Председатель ЦМК _____ Кирилюк Н.В.

СОГЛАСОВАНО
Зам. декана по учебной работе
_____ А.А. Санова
«27» 05 2021 г.

СОГЛАСОВАНО
Научная библиотека
_____
«27» 05 2021 г.

1. Область применения программы

2.

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 является частью образовательной программы в соответствии с ФГОС по специальности СПО Обеспечение информационной безопасности телекоммуникационных системах.

Рабочая программа может быть использована в дополнительном профессиональном образовании.

3. Место учебной дисциплины в структуре основной образовательной программы:

ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средствах защиты относится к дисциплинам профессиональных модулей, читается в 3, 4 5, 6 семестрах в объеме 944 акад.часа с учетом практики, в том числе 980 акад.час.

На компетенциях, формируемых на профессиональном модуле базируется прохождение производственной практики и производственной практики (преддипломной), а также подготовка и защита выпускной квалификационной работы.

4. Показателем освоения профессионального модуля:

Результатом освоения профессионального модуля является овладение профессиональными (ПК) и общими (ОК) компетенциями:

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 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

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 предъявляемыми требованиями.

В результате освоения профессионального модуля обучающийся должен иметь практический опыт:

- применения программно-аппаратных средств обеспечения информационной безопасности;
- диагностики, устранение отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;
- мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;
- обеспечение учета, обработки, хранения и передачи конфиденциальной информации;
- решение частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
- применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.

В результате освоения профессионального модуля обучающийся должен уметь:

- применять программно-аппаратные средства обеспечения информационной безопасности;
- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
- оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
- участвовать в обеспечение учета, обработки, хранения и передачи конфиденциальной информации;
- решать частые технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;
- использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

В результате освоения профессионального модуля обучающийся должен знать:

- методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
- особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
- типовые модели управления доступом;
- типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- типовые средства и методы ведения аудита и обнаружение вторжений;
- типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
- основные понятия криптографии и типовые криптографические методы защиты информации.

5. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Тематический план профессионального модуля

Код профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Консультации, часов	Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося			Производственная (по профилю специальности), ** часов	
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов			
1	2	3	4	5	6	7	8	9	10	
ПК 2.1-2.3	**МКД.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты**	**407**	**329**	152	-	**44**	20	**34**	**-**	
ПК 2.1-2.3	**МДК.02.02 Криптографическая защита информации**	**345**	**265**	118	-	**46**	20	**34**	**-**	
ПК 2.1-2.3	**УП.02.01 Учебная практика**	**72**						**-**	**-**	
ПК 2.1-2.3	**ПП.01.01 Производственная практика**	**108**						**-**	**108**	
	Всего:	**944**	**786**	270	-	**90**	-	**68**	**108**	

4.2 Тематический план и содержание ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средствах защиты

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	Уровень усвоения
1	**2**	**3**	
ПМ.02.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты			
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание**	26	1,2
	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. WindowsXP. 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 работы	**86**	
	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав пользователя	6	
	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	6	

	Настройка изолированной среды	4	
	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	4	
	Лабораторные работы		
	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация	4	
	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	4	
	Восстановление информации типовыми средствами Программы восстановление информации	4	
Тема 1.2. Технологии разграничения доступа	**Содержание**		
	Архитектура подсистемы защиты операционной системы Windows Server2016. Особенности ОС Windows Server2016. 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 возможности 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.	**26**	2
	Практические работы	**60**	
	Программы надежного удаления информации	4	
	Архивирование информации	4	
	Лабораторные работы		
	Программные средства резервного копирования. Настройка RAID-массивов	4	
	Инсайдерская информация. Программы сбора информации о ПК	4	
	Настройка межсетевого экрана.	4	
Тема 1.3. Обеспечение	**Содержание**	**28**	

информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP.Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. 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. Тунелирование. 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.		2,3
	Практические работы	36	
	Основные действия с виртуальной машиной	6	
	Работа с контрольными точками	6	
	Использование внешних устройств	6	
	Работа с локальным хранилищем сертификатов в ОС WINDOWS	6	
	Установка и настройка ПО	6	
	Настройка ПО с помощью групповых политик	6	
	Развертывание TMS в среде Active Directory	6	
	Настройка TMS всреде Active Directory	6	
	Настройкаполитик TMS	6	
	Лабораторные работы		
	Настройка использования виртуального токена	4	
	Использование токена на рабочем месте администратора	4	
	Установка и настройка драйверов	4	
	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	4	
	Применение DallasLock	4	
	Применение MaxPatrolEducation	4	
	Изучение основных возможностей ПО	4	
	Изучение настроекПО	4	
	Изучение возможностей ПО Деловая почта	4	

Тема 1.4. Технологии обнаружения вторжений	**Содержание**		**2,3**
	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 вирусовЖизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.	**26**	
	Практические работы	**16**	
	Изучение средств обнаружения атак	4	
	Лабораторные работы		
	Изучение антивирусных продуктов	6	
Тема 1.5. Методы управления средствами защиты	**Содержание**		2,3
	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.	**24**	
Курсовой проект (работа) **Тематика курсовых проектов (работ):** 1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей. 2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей. 3. Анализ методов и средств анализа защищенности беспроводных сетей. 4. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения. 5. Виброакустические средства современных систем обеспечения информационной безопасности. 6. Средства защиты от ПЭМИН, современное состояние, проблемы и решения. 7. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 8. Средства обеспечения информационной безопасности банков данных.		20	

9. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса). 10. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации. 11. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 12. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 13. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 14. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 15. Инструментальные средства анализа рисков информационной безопасности. 16. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками. 17. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).		
Внеаудиторная (самостоятельная) учебная работа при изучении раздела ПМ	44	
Рекомендуемая примерная тематика самостоятельной работы для разработчиков программ образовательной организации: 1. Проблемы обеспечения безопасности операционных системWindowsXP. Windows 7. Windows8. Linux. QNX. 2.Технологии аутентификации. 3.Аутентификация, авторизация и администрирование действий пользователя. 4.Пароли. PIN-коды. Методы надежного составления паролей. 5.Токены. Смарт-карты. Виртуальные ключи. 6.Программно-аппаратные модули доверенной загрузки. 7.АПМДЗ Криптон –Замок системный администратор. 8.Изучение настроек системного администратора АПМДЗ. 9.Сектор НЖМД. Область памяти. Файл, папка, каталог. 10. Разграничение доступа к объектам операционной системы. 11. Комплексная система организации управления доступом. Инсталяция. Настройка. 12.Аудит безопасности операционной системы. 13.Функции межсетевых экранов.Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. 14.Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. 15.Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. 16.Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. 17. Концепция построения виртуальных защищенных сетей;. 18. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура защищенного пакета. Варианты построения защищенных каналов. 19. Защита на канальном уровне.ПротоколыPPTP, L2F, L2TP. 20. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. 21.Защита на сетевом уровне.Архитектура средств безопасности IPSec, AH, ESP. 22.Защита на прикладном уровне. ПротоколыPAP, CHAP,S/Key, SSO, Kerberos. 23.Функционирование системы управления средствами защиты. 24.Аудит безопасности информационной системы.		
Консультации	34	
Раздел 2.Криптографическая защита информации		
МДК 02.02.Криптографическая защита информации		

Тема 2.1. Основы криптографических методов защиты информации	**Содержание**		
	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.	**36**	2,3
	Практические работы	**58**	
	Стеганографические методы скрытия информации	6	
	Бинарная арифметика. Модульная арифметика	6	
	Применение методов шифрования перестановкой	6	
	Применение методов шифрования заменой	6	
	Лабораторные работы		
	Применение методов шифрования многоалфавитной замены	4	
	Криптоанализ методов перестановки	4	
	Криптоанализ методов замены	6	
	Компьютерное шифрование	4	
Тема 2.2. Современные	**Содержание**	**38**	**2,3**

стандарты шифрования	Симметричное шифрование. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES. Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES. Российские стандарты симметричного шифрования . Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. Проблема распределения ключей симметричного шифрования. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. Асимметричное шифрование. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП. Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.		
	Практические работы	**40**	
	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	6	
	Лабораторные работы		
	Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	4	
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	**Содержание**	**36**	2,3
	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. 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 34.10 -2012. Установление подлинности объекта. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. Проблемы распределения открытого ключа асимметричного шифрования. Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. Электронная почта. Архитектура e-mail. PGP. S/M1ME . Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети		

	Защита информации в сетях организованных по технологии беспроводного доступа. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16. Защита информации в сетях сотовой связи. А3. А8.А5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи. Криптовалюты. Биткоин. Блокчейн-системы Ethereum. Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.		
	Практические работы	**62**	
	Разработка хэш-функции	6	
	Разработка схемы простого пароля	6	
	Разработка схемы динамического пароля	6	
	Сертификаты открытого ключа	6	
	Настройка и администрирование токена	6	
	Настройка сервисов Рутокен-PinPad	6	
	Лабораторные работы		
	Настройка сервисов Рутокен-ЭЦП	6	
	Настройка сервисов Рутокен–Bluetooth	6	
	Настройка сервисов Рутокен–S	6	
	Разработка алгоритма PGP	4	
	Изучение протоколов SSL, TLS, IPSec	4	
	Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	4	
Курсовой проект (работа) **Тематика курсовых проектов (работ):** 1. Модель угроз НСД на предприятии 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии 6. Построение модели нарушителя по требованиям ФСБ на предприятии 7. Модель угроз безопасности ИС персональных данных на предприятии 8. Комплексная модель защиты информации на предприятии. 9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся		**20**	

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.		
Самостоятельная учебная работа при изучении раздела ПМ	**46**	
Рекомендуемая тематика внеаудиторной (самостоятельной0 работы: 1. Изучение новых технологий хранения информации. 2. Статистика и анализ крупных утечек информации за год. 3. Поиск информации о новых видах атак на информационную систему. 4. Обзор современных программных и программно-аппаратных средств защиты. 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты. 6. Криптографические методы. 7. Шифрование. Кодирование. Стеганография. Сжатие. 8. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. 9. Традиционные шифры замены. Шифры многоалфавитной замены. Частотность символов. 10. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. 11. Компьютерное шифрование. 12. Стандарт шифрования данных DES. Структура DES. Безопасность DES. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. 13. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. 14. Асимметричное шифрование. Криптографическая система Эль-Гамаля. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.		
Консультации	**34**	
Промежуточная аттестация	**54**	
Учебная практика **Виды работ** Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции Составление алгоритма шифра Подключение, установка драйверов, настройка программных средств шифрования Криптон. Администрирование программных средств шифрования Криптон Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. Администрирование аппаратных средств шифрования Криптон.	**72**	

Производственная практика **Виды работ** Участие в организации работ по защите персональных компьютеров на предприятии Участие в организации работ по защите локальных сетей на предприятии Участие в организации работ по защите работ в глобальной сети интернет на предприятии Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. Администрирование систем безопасности проводной защищенной локальной сети. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. Администрирование систем безопасности беспроводной защищенной локальной сети. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей Подключение, установка драйверов, настройка программных средств абонентского шифрования Администрирование внедренных средств Настройка средств электронной подписи Администрирование средств электронной подписи Администрирование средств PKI	**108**	
Всего (с учетом практики)	**980**	

6. Образовательные технологии

Результаты освоения профессионального модуля достигаются за счет использования в процессе обучения современных инструментальных средств: лекции с применением мультимедийных технологий, практические занятия с использованием соответствующего оборудования.

При проведении занятий используются активные и интерактивные формы. В таблице приведено описание образовательных технологий, используемых в данном модуле.

Методы и формы организации обучения (ФОО)

МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

ФОО / Методы	Лекция	Пр.раб
Работа в команде		Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN
Беседа	Тема 1.1. Обеспечение безопасности операционных систем	

МДК.02.02 Криптографическая защита информации

ФОО / Методы	Лекция	Пр.раб
Работа в команде		Тема 2.2. Современные стандарты шифрования
Беседа	Тема 2.1. Основы криптографических методов защиты информации	

7. Требования к минимальному материально-техническому обеспечению

Занятия по профессиональному модулю проводятся в учебной аудитории, компьютерном классе, лаборатории информационно-телекоммуникационных систем и сетей, лаборатории защиты информации от утечки по техническим каналам, лаборатории программных и программно-аппаратных средств защиты информации, кабинете метрологии и стандартизации

Оснащения кабинета:Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: учебная мебель, доска, мультимедиа-проектор, проекционный экран, ПК.

Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: учебная мебель, доска, мультимедиа-проектор, проекционный экран, ноутбук. Лабораторное оборудование.

Оснащение лаборатории:Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: учебная мебель, ПК Intel 3GHz, 4GBRAM, 300 GBHDD, 22”LCD-11 шт.; СЗИ НСД Аккорд АМД 3 -6шт.; Сервер Depo Strom-1 шт.; Ревизор сети 2.0 -система анализа программного обеспечения сетей TCP/IP - 5шт.; Коммутатор 1Gb Ethernet управляемый 16 портов -DES-3200-18 - 1 шт.; Страж NTv.3.0 – 5шт; Консоль стоечная 19” AtenSlideawaiLCDConsolemasterview 1 шт. ; Terrier v.3.0 – 5шт.; Стойка серверная 19” защищенная – 1 шт.; Ревизор 1 XP – 5шт.; ИБП – SmartUPS 1500 - 1 шт.;

Ревизор 2 XP – 5шт.; Лавина СКУД – комплекс для программирования карт; Фикс 2.0.1 – 5шт.; Платы расширения SecretNetCard – 5шт; НСД DallasLock 8.0; ПАК соболь в.3.0. – 5шт.; НСД SecretNetStudio

8. Учебно-методическое и информационное обеспечение дисциплины

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Новожилов, О. П. Информатика в 2 ч. Часть 1 : учебник для среднего профессионального образования / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 320 с. — (Профессиональное образование). — ISBN 978-5-534-06372-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/448995

2. Новожилов, О. П. Информатика в 2 ч. Часть 2 : учебник для среднего профессионального образования / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 302 с. — (Профессиональное образование). — ISBN 978-5-534-06374-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/448996

3. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456638

4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933

Дополнительная литература

5. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356

6. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792

7. Гаврилов, М. В. Информатика и информационные технологии : учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 383 с. — (Профессиональное образование). — ISBN 978-5-534-03051-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449286

8. Разработка и защита баз данных в Microsoft SQL Server 2005 : учебное пособие для СПО / . — Саратов : Профобразование, 2019. — 148 с. — ISBN 978-5-4488-0366-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86207.html

9. Никифоров, С. Н. Защита информации. Пароли, скрытие, удаление данных : учебное пособие / С. Н. Никифоров, М. М. Ромаданов. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ,

2017. — 108 c. — ISBN 978-5-9227-0783-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/80747.html

10. Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 с. — ISBN 978-5-9227-0757-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/74381.html

11. Никифоров, С. Н. Защита информации. Защищенные сети : учебное пособие / С. Н. Никифоров. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 80 с. — ISBN 978-5-9227-0762-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/74382.html

12. Зиангирова, Л. Ф. Инфокоммуникационные системы и сети : учебное пособие для СПО / Л. Ф. Зиангирова. — Саратов : Профобразование, Ай Пи Ар Медиа, 2019. — 128 с. — ISBN 978-5-4488-0302-4, 978-5-4497-0183-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/85806.html

13. Хаулет, Т. Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям : учебное пособие / Т. Хаулет ; перевод В. Галатенко, О. Труфанова ; под редакцией В. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 607 с. — ISBN 978-5-4497-0658-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97544.html

14. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средствах защиты [Электронный ресурс] : сб. учеб.-метод. материалов спец. 10.02.04 "Обеспечение информ. безопасности телекоммуникац. систем" / АмГУ, ФСПО ; сост. В. В. Санов. - Благовещенск : Изд-во Амур. гос. ун-та, 2018. - 12 с. — Режим доступа: http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/10138.pdf

Перечень программного обеспечения

Операционная система WindowsServer 2008 - DreamSparkPremiumElectronicSoftwareDeliveryRenewal по договору - Субли-цензионный договор № Tr000074357/KHB 17 от 01 марта 2016 года, Операционная система MS Windows XP SP3 - DreamSparkPremiumElectronicSoftwareDeliveryRenewal по договору - Субли-цензионный договор № Tr000074357/KHB 17 от 01 марта 2016 года

Операционная система MSWindows 7 Pro - DreamSparkPremiumElectronicSoftwareDeliveryRenewal по договору - Сублицензионный договор № Tr000074357/KHB 17 от 01 марта 2016 года

8. Контроль и оценка результатов освоения учебной дисциплины

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты (освоенные профессиональные компетенции)	**Формы и методы контроля и 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	экспертная оценка выполнения практической работы установке программного обеспечения

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.	Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения
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 предъявляемыми требованиями.	Текущий контроль в форме: - защиты практических занятий; - контрольных работ по темам МДК. Зачеты по учебной практике и по разделу профессионального модуля. Дифференцированный зачёт по профессиональному модулю.
Промежуточная аттестация	**Другие формы контроля, Курсовая работа, курсовой проект, дифференцированный зачет, экзамен по модулю**