ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

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
(наименование учебной дисциплины)

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код, наименование профессии/специальности)

2024

Рассмотрено и согласовано цикловой комиссией компьютерных дисциплин.

Протокол № 2 от «02» сентября 2024 г.

Разработана на основе ФГОС СПО РФ и ПООП СПО для специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» (утверждён приказом Министерства образования и науки от 9 декабря 2016 №1551).

Организация разработчик: Политехнический колледж ЛГАУ

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

1.1. Область применения программы профессионального модуля

Рабочая программа профессионального модуля (далее – рабочая программа) является частью освоения программ подготовки специалистов среднего звена (далее ППССЗ) в соответствии с ФГОС СПО РФ и ПООП СПО для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

(указать профессию, специальность, укрупненную группу (группы) профессий или направление (направления) подготовки)

Рабочая программа профессионального модуля ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем может быть использована на базе среднего (полного общего) образования, в профессиональном обучении и дополнительном профессиональном образовании.

1.2. Цели и задачи профессионального модуля, требования к результатам освоения профессионального модуля

В результате изучения профессионального модуля студент должен

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;

В результате освоения изучения профессионального модуля студент должен **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;

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения рабочей программы профессионального модуля является овладение обучающимся видом профессиональной деятельности, в том числе профессиональными (ПК) и общими (ОК) компетенциями в соответствии с требованиями Федерального Государственного образовательного стандарта среднего профессионального образования Российской Федерации по специальности среднего профессионального образования 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Код	Наименование результата обучения
ВД 1	**Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты**
ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.

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

Всего – 882 часа, в том числе
максимальной учебной нагрузки обучающихся – 850 часов,
включая:
обязательной аудиторной учебной нагрузки обучающихся –670 часов;
самостоятельной работы обучающихся – 196 часов;
учебной и производственной практики –168 часа.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

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

Коды профессиональных компетенций	**Наименование разделов профессионального модуля**	**Всего часов**[1]	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**				**Практика Учебная, (по профилю специальности),** часов	**зачет, дифференцированный зачет**	**Консультации**	**Экзамен, Квалификационный экзамен**
			Обязательная аудиторная учебная нагрузка учащихся			**Самостоятельная работа учащихся,** часов				
			лекции	**лабораторные работы и практические занятия,** часов	**курсовая работа (проект),** часов					
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***
	ПМ.02 Защита инф в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	**16**							4	12
ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10	МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	**415**	80	164	46	117	-	-	2	6
ПК 2.1 - 2.3 ОК 01-04,	МДК 02.02.Криптографическая защита информации	**292**	80	119	–	85	-		2	6
ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10	Учебная практика, часов	**108**	–	–	–	–	102	6	-	-
ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10	Производственная практика, часов	**72**	–	–	–	–	66	6	-	-
	Всего часов:	**903**	**160**	**283**	**46**	**202**	**168**	**12**	**8**	**24**

[1] Колонка *3* – это сумма колонок *4, 7, 9,10*

3.2. Содержание обучения 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

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
ПМ.02.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты		**903**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**415**	
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**415**	
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание учебного материала**	**74**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	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.	16	
	Практическое занятие. Инструктаж по ТБ Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя. Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита. Настройка изолированной среды. АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды. Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация. Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование. Восстановление информации типовыми средствами Программы восстановление информации.	34	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
	Самостоятельная работа обучающихся: Проблемы обеспечения безопасности операционных системWindowsXP. Windows 7. Windows8. Linux. QNX. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя. Пароли. PIN-коды. Методы надежного составления паролей. Токены. Смарт-карты. Виртуальные ключи. Программно-аппаратные модули доверенной загрузки. АПМДЗ Криптон –Замок системный администратор.	24	
Тема1.2.Технологии разграничения доступа	**Содержание учебного материала**	**74**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	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.	16	
	Практическое занятие. Инструктаж по ТБ Программы надежного удаления информации. Архивирование информации. Программные средства резервного копирования. Настройка RAID-массивов. Инсайдерская информация. Программы сбора информации о ПК. Настройка межсетевого экрана. 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.	34	
	Самостоятельная работа обучающихся: Изучение настроек системного администратора АПМДЗ. Сектор НЖМД. Область памяти. Файл, папка, каталог. Разграничение доступа к объектам операционной системы. Комплексная система организации управления доступом. Инсталяция. Настройка. Аудит безопасности операционной системы. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная	24	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
	фильтрация. Посреднические функции. Дополнительные возможности МЭ.		
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание учебного материала**	**74**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	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.	16	
	Практическое занятие. Инструктаж по ТБ 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 всреде Active Directory. Настройкаполитик TMS. Настройка использования виртуального токена. Использование токена на рабочем месте администратора. Установка и настройка СКЗИ «КриптоПроCSP». Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP. Применение SecretDisk4. Применение SecretDisk Server NG. Изучение основных возможностей ПО VipNetClient. Изучение настроекПОVipNetClient. Изучение возможностей ПО Деловая почта.	34	
	Самостоятельная работа обучающихся: Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. Концепция построения виртуальных защищенных сетей;. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура защищенного пакета. Варианты построения защищенных каналов. Защита на канальном уровне.ПротоколыPPTP, L2F, L2TP.	24	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
Тема1.4. Технологии обнаружения вторжений	**Содержание учебного материала**	**74**	
	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.	16	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	Практическое занятие. Инструктаж по ТБ Изучение средств обнаружения атак Изучение антивирусных продуктов. 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.	34	
	Самостоятельная работа обучающихся 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. ПротоколыPAP, CHAP,S/Key, SSO, Kerberos.	24	
Тема 1.5. Методы управления средствами защиты	**Содержание учебного материала**	**54**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы.	12	
	Практическое занятие. Инструктаж по ТБ 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	
	Самостоятельная работа обучающихся Функционирование системы управления средствами защиты. Аудит безопасности информационной системы. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ.	18	
Курсовой проект (работа) **Тематика курсовых проектов (работ):** 1.Модель угроз НСД на предприятии 2.Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии		**46**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
	3.Проведение классификации ПО по требованиям ФСТЭК на предприятии 4.Проведение классификации МЭ по требованиям ФСТЭК на предприятии 5.Построение модели нарушителя по требованиям ФСТЭК на предприятии 6.Построение модели нарушителя по требованиям ФСБ на предприятии 7.Модель угроз безопасности ИС персональных данных на предприятии 8.Комплексная модель защиты информации на предприятии. 9.Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 10.Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 11.Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 12.Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 13.Проблема защиты информации в облачных хранилищах данных и ЦОДах 14.Защита сред виртуализации.		
	Всего: **из них: практических занятий** **курсовой проект** **лекций** **самостоятельная работа** **консультация** **экзамен**	**415** **164** **46** **80** **117** **2** **6**	
Раздел 2.Криптографическая защита информации		**292**	
МДК 02.02.Криптографическая защита информации		**292**	
Тема 2.1. Основы криптографических методов защиты информации	**Содержание учебного материала**	**92**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	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.	19	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
	Практическое занятие. Инструктаж по ТБ Стеганографические методы скрытия информации. Бинарная арифметика. Модульная арифметика. Применение методов шифрования перестановкой. Применение методов шифрования заменой. Применение методов шифрования многоалфавитной замены. Криптоанализ методов перестановки. Криптоанализ методов замены. Компьютерное шифрование. 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.	54	
	Самостоятельная работа обучающихся Изучение новых технологий хранения информации. Статистика и анализ крупных утечек информации за год. Поиск информации о новых видах атак на информационную систему. Обзор современных программных и программно-аппаратных средств защиты. Сравнительный анализ современных программных и программно-аппаратных средств защиты	28	
Тема 2.2. Современные стандарты шифрования	**Содержание учебного материала**	**92**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	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.	26	
	Самостоятельная работа обучающихся Криптографические методы. Шифрование. Кодирование. Стеганография. Сжатие. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Традиционные шифры замены. Шифры многоалфавитной замены. Частотность символов. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста.	28	
Тема 2.3. Криптографические методы обеспечения безопасности	**Содержание учебного материала**	**4**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	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	32	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
сетевых технологий	подписи. Ата- ки 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.		
	Практическое занятие. Инструктаж по ТБ Разработка хэш-функции. Разработка схемы простого пароля. Разработка схемы динамического пароля. Сертификаты открытого ключа. Настройка и администрирование токена. Настройка сервисов Рутокен-PinPad. Настройка сервисов Рутокен-ЭЦП. Настройка сервисов Рутокен–Bluetooth. Настройка сервисов Рутокен–S. Разработка алгоритма PGP. Изучение протоколов SSL, TLS, IPSec. Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2. 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. A3. A8.A5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи. Криптовалюты. Биткоин. Блокчейн-системы Ethereum. Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асиммет- ричных алгоритмов.	61	
	Самостоятельная работа обучающихся Компьютерное шифрование. 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. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. Асимметричное шифрование. Криптографическая система Эль-Гамаля. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.	26	
	Всего: **из них: практических занятий** **лекций** **самостоятельная работа**	**292** **119** **80** **85**	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
	консультация **экзамен**	**2** **6**	
Учебная практика УП.02 **Виды работ:** – Выбор, подключение, настройка межсетевого крана. Администрирование межсетевого экрана. – Ознакомление, подключение, настройка системы резервного копирования Администрирование системы резервного копирования. – Ознакомление, подключение, настройка системы антивирусной защиты. – Администрирование системы антивирусной защиты. – Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции Составление алгоритма шифра – Подключение, установка драйверов, настройка программных средств шифрования Криптон. Администрирование программных средств шифрования Криптон – Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. – Администрирование аппаратных средств шифрования Криптон.		**102**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10
	Дифференцированный зачет	**6**	
Производственная практика ПП.02 **Виды работ:** Защита информации от несанкционированного доступа Регистрация и учёт входа/выхода субъектов системы в/из системы (узла сети) Учёт носителей информации Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей Работа с антивирусами Обновление антивирусных программ Защита почтовых ящиков Шифрование конфиденциальной информации Работа в программе cryptoapi Работа в программе Windows Defender Изучение дискреционного принципа контроля доступа к информации Создание системы защиты персональных данных Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ		**66**	ПК 2.1 - 2.3 ОК 01-04, ОК 9, ОК10

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Осваиваемые элементы компетенций
	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 Работа с криптографическими средствами защиты информации 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. 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 Сдача рабочего места Подготовка дневника и аттестационного листа по практике Подготовка и сдача отчета по практике		
	Дифференцированный зачет	**6**	
	Консультация	**4**	
	Квалификационный экзамен	**12**	
Всего по ПМ.02		**903**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Требования к материально-техническому обеспечению

Реализация программы дисциплины требует наличия лаборатории «Защиты информации от утечки по техническим каналам».

Эффективность преподавания профессионального модуля зависит от наличия соответствующего материально-технического оснащения. Это объясняется особенностями курса, в первую очередь его многопрофильностью и практической направленностью.

Лаборатория «Защиты информации от утечки по техническим каналам», должна быть оснащена средствами защиты информации от утечки по акустическому (виброакустическому) каналу; средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок;

- шумогенераторы;
- комплексный поисковый прибор;
- прожигатели телефонных линий;
- устройство обнаружения скрытых видеокамер;
- виброакустические генераторы;
- подавители диктофонов;
- подавители устройств сотовой связи;
- устройство защиты аналоговых сигналов;
- устройство защиты цифровых сигналов;

Требования к квалификации педагогических кадров, осуществляющих реализацию ППССЗ по специальности, должны обеспечиваться педагогическими кадрами, имеющими среднее профессиональное, высшее образование, соответствующее профилю преподаваемой учебной дисциплины. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального учебного цикла.

Преподаватели получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже одного раза в 5 лет.

4.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Печатные издания

1. 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.

2. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов, 5-е изд. – Спб.: Питер, 2015. – 944 с.

3. Томаси У. Электронные системы связи.- М.: Техносфера, 2016. - 1360с.

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.

5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013. – 172 с.

6. 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

7. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

9. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение инфор- мационной безопасности: учебник: Рекомендовано УМО, 2009. - 192с.

10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Электронные издания (электронные ресурсы)

Интернет-ресурсы:

11. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

12. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

13. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

14. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
1	2
Умения	
– 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;	Контроль знаний и умений осуществляется в ходе выполнения практических и лабораторных работ, промежуточной аттестации. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы Экспертное заключение преподавателя
Знания:	
– 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;	Контроль выполняется по результатам проведения различных форм опроса, выполнения контрольных работ, тестирования, выполнения практических работ, промежуточной аттестации. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы

`Приложение 1

ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ К.Е. ВОРОШИЛОВА»

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА
профессионального модуля

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

(наименование учебной дисциплины)

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

(код, наименование профессии/специальности)

2024

Задания к экзамену по ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе криптографических средств защиты

Задание 1. Выполните настройку программных и программно-аппаратных средств защиты информации для обеспечения защиты информации в информационно-телекоммуникационных системах и сетях

1. Задача по настройке безопасности ОС Windows:
• Шаг 1: Установить ОС Windows на виртуальную машину.
• Шаг 2: Настроить политику паролей и блокировку экрана.
• Шаг 3: Настроить антивирусную программу и запланировать ежедневную проверку системы.
• Шаг 4: Настроить межсетевой экран и открыть только необходимые порты.
• Шаг 5: Настроить обновления ОС и приложений для устранения уязвимостей.
• Шаг 6: Запланировать резервное копирование данных.

2. Разработка модели безопасности на основе мандатной политики:
• Шаг 1: Определить уровни доступа пользователей и объектов в системе.
• Шаг 2: Создать таблицу доступа, определяющую права доступа пользователей к объектам системы.
• Шаг 3: Настроить политику безопасности на основе созданной таблицы.
• Шаг 4: Создать пользователя и проверить права доступа.

3. Разработка модели безопасности на основе ролевой политики:
• Шаг 1: Определить роли пользователей и объекты, к которым они имеют доступ.
• Шаг 2: Создать таблицу ролей, определяющую связь между ролями и объектами системы.
• Шаг 3: Настроить политику безопасности на основе созданной таблицы.
• Шаг 4: Создать пользователя и назначить ему роль.

4. Резервирование данных:
• Шаг 1: Определить данные, которые требуется резервировать.
• Шаг 2: Выбрать программное обеспечение для резервного копирования.
• Шаг 3: Настроить расписание резервного копирования.
• Шаг 4: Проверить корректность резервного копирования.

5. Разграничение доступа в ОС Windows:
• Шаг 1: Создать группы пользователей и назначить им права доступа.
• Шаг 2: Создать пользователей и назначить их в нужные группы.
• Шаг 3: Настроить права доступа к файлам и папкам.

• Шаг 4: Проверить корректность настроек.

6. Настройка межсетевого экрана:
• Шаг 1: Определить правила доступа к сети.
• Шаг 2: Настроить правила фильтрации пакетов и доступа к определенным портам
Шаг 3: Настроить список исключений.
Шаг 4: Проверить работоспособность межсетевого экрана.

7. Настройка VPN:
• Шаг 1: Установить и настроить VPN-сервер.
• Шаг 2: Создать профили пользователей и назначить им права доступа.
• Шаг 3: Настроить шифрование трафика и сертификаты безопасности.
• Шаг 4: Проверить работу VPN-соединения.

8. Настройка системы обнаружения вторжений:
• Шаг 1: Установить и настроить систему обнаружения вторжений (IDS/IPS).
• Шаг 2: Создать правила обнаружения вторжений и исключения.
• Шаг 3: Настроить оповещение о возможных атаках.
• Шаг 4: Проверить работу системы обнаружения вторжений.

9. Организация защиты компьютерной системы:
• Шаг 1: Оценить уязвимости компьютерной системы.
• Шаг 2: Установить и настроить необходимое программное и аппаратное обеспечение.
• Шаг 3: Разработать стратегию бэкапирования и резервного копирования данных.
• Шаг 4: Провести тестирование на проникновение.

10. Настройка отделов и групповых политик в DLP-системе Search Inform:
• Шаг 1: Создать группы пользователей и отделов.
• Шаг 2: Настроить правила обнаружения и контроля передачи конфиденциальных данных.
• Шаг 3: Настроить мониторинг и оповещение о нарушениях безопасности.
• Шаг 4: Проверить работоспособность системы DLP.

11. Настройка системы обнаружения вторжений:
• Шаг 1: Установить программу системы обнаружения вторжений (например, Snort).
• Шаг 2: Создать файл конфигурации программы.
• Шаг 3: Настроить правила обнаружения вторжений.
• Шаг 4: Проверить работу программы на тестовой среде.

12. Организация защиты компьютерной системы:
• Шаг 1: Оценить уязвимости системы.
• Шаг 2: Установить антивирусное программное обеспечение.
• Шаг 3: Настроить правила межсетевого экрана.
• Шаг 4: Настроить систему обнаружения вторжений.
• Шаг 5: Настроить резервное копирование данных.
• Шаг 6: Провести обучение пользователей вопросам информационной безопасности.

13. Настройка отделов и групповых политик в DLP-системе Search Inform:
• Шаг 1: Установить программу DLP-системы Search Inform.
• Шаг 2: Создать отделы и группы пользователей.
• Шаг 3: Настроить права доступа для каждой группы пользователей.
• Шаг 4: Настроить правила мониторинга и блокировки данных в соответствии с требованиями компании.
• Шаг 5: Проверить работу системы на тестовых данных.

14. Настройка безопасности Wi-Fi-сети:
• Шаг 1: Определить тип шифрования и установить его.
• Шаг 2: Настроить пароль доступа к сети.
• Шаг 3: Ограничить доступ к сети по MAC-адресам устройств.
• Шаг 4: Проверить корректность настроек.

15. Разработка политики удаленного доступа к серверам:
• Шаг 1: Определить список пользователей и их права доступа.
• Шаг 2: Настроить удаленный доступ по протоколу SSH.
• Шаг 3: Ограничить доступ по IP-адресам.
• Шаг 4: Проверить корректность настроек.

16. Настройка системы антивирусной защиты:
• Шаг 1: Установить антивирусное ПО на компьютер.
• Шаг 2: Настроить автоматические проверки файлов и директорий.
• Шаг 3: Настроить автоматические обновления антивирусной базы данных.
• Шаг 4: Проверить корректность настроек.

17. Разработка механизма резервного копирования данных:
• Шаг 1: Определить список файлов и директорий для резервного копирования.
• Шаг 2: Выбрать метод резервного копирования (полный, инкрементальный, дифференциальный).
• Шаг 3: Настроить расписание резервного копирования.
• Шаг 4: Проверить корректность настроек.

18. Настройка механизма шифрования файлов:
• Шаг 1: Установить ПО для шифрования файлов.
• Шаг 2: Создать ключ шифрования.
• Шаг 3: Настроить права доступа к зашифрованным файлам.
• Шаг 4: Проверить корректность настроек.

19. Разработка политики безопасности сетевых служб:
• Шаг 1: Определить список сетевых служб, доступных для использования.
• Шаг 2: Определить список пользователей и их права доступа к сетевым службам.
• Шаг 3: Ограничить доступ к сетевым службам по IP-адресам.
• Шаг 4: Проверить корректность настроек.

20. Настройка протоколирования событий в ОС Windows:
• Шаг 1: Открыть центр управления безопасностью.
• Шаг 2: Выбрать опцию "Аудит событий".
• Шаг 3: Настроить параметры протоколирования событий в соответствии с требованиями безопасности.
• Шаг 4: Проверить правильность настроек.

21. Настройка системы контроля целостности файлов:
• Шаг 1: Установить программу контроля целостности файлов, например, Tripwire.
• Шаг 2: Создать базу данных для хранения информации о контролируемых файлах.
• Шаг 3: Настроить систему для контроля целостности файлов.
• Шаг 4: Проверить работу системы контроля целостности файлов.

22. Разработка и настройка системы шифрования данных:
• Шаг 1: Выбрать программное обеспечение для шифрования данных, например, VeraCrypt.
• Шаг 2: Установить и настроить программу шифрования.
• Шаг 3: Создать зашифрованный том для хранения данных.
• Шаг 4: Проверить правильность настроек системы шифрования.

23. Настройка системы контроля доступа к сетевым ресурсам:
• Шаг 1: Выбрать программное обеспечение для контроля доступа к сетевым ресурсам, например, Access Manager.
• Шаг 2: Установить и настроить программу контроля доступа к сетевым ресурсам.
• Шаг 3: Создать правила доступа для пользователей и групп пользователей.

• Шаг 4: Проверить работу системы контроля доступа к сетевым ресурсам.

24. Разработка и настройка системы мониторинга безопасности:

• Шаг 1: Выбрать программное обеспечение для мониторинга безопасности, например, Security Center.

• Шаг 2: Установить и настроить программу мониторинга безопасности.

• Шаг 3: Создать правила мониторинга для обнаружения угроз безопасности.

• Шаг 4: Проверить работу системы мониторинга безопасности.

25. Настройка биометрической аутентификации в ОС Windows 10:

• Шаг 1: Проверить поддерживается ли ваше устройство считывания биометрических данных в Windows 10.

• Шаг 2: Настроить устройство считывания в драйверах Windows.

• Шаг 3: Настроить параметры аутентификации через биометрию.

• Шаг 4: Проверить работоспособность аутентификации через биометрию.

Задание 2. Выполните настройку криптографических средств защиты информации для обеспечения защиты информации в информационно-телекоммуникационных системах и сетях

1. Установите VipNet/SecretNet на сервер и настройте его для работы в вашей сети.

2. Настройте аутентификацию пользователей VipNet/SecretNet через Active Directory.

3. Создайте политики безопасности для VipNet/SecretNet, чтобы ограничить доступ к ресурсам сети только для авторизованных пользователей.

4. Настройте шифрование данных для всех трафика, проходящего через VipNet/SecretNet.

5. Настройте VipNet/SecretNet для работы в режиме "туннельного" шифрования, чтобы защитить данные, передаваемые через открытые сети, такие как Интернет.

6. Настройте фильтрацию трафика, чтобы блокировать попытки неавторизованного доступа к сети.

7. Настройте мониторинг и журналирование для VipNet/SecretNet, чтобы отслеживать любые попытки нарушения безопасности.

8. Настройте систему уведомлений, чтобы быстро реагировать на любые попытки нарушения безопасности.

9. Создайте профили пользователей для управления доступом к ресурсам в вашей сети.

10. Настройте группы пользователей для легкого управления доступом к ресурсам.

11. Настройте политики паролей для VipNet/SecretNet, чтобы гарантировать, что все пароли сложны и изменяются регулярно.

12. Настройте функцию блокировки пользователей, чтобы предотвратить неудачные попытки аутентификации.

13. Создайте отчеты об активности пользователей, чтобы отслеживать любые подозрительные действия.

14. Настройте механизмы защиты от DDoS-атак для VipNet/SecretNet.

15. Настройте механизмы защиты от ARP-атак для VipNet/SecretNet.

16. Настройте механизмы защиты от IP-атак для VipNet/SecretNet.

17. Настройте функцию восстановления после сбоя, чтобы быстро вернуть VipNet/SecretNet к работе в случае сбоя или отказа.

18. Настройте функцию резервирования, чтобы обеспечить непрерывную работу VipNet/SecretNet в случае отказа оборудования.

19. Настройте VipNet/SecretNet для работы с другими средствами защиты информации, такими как антивирусное программное обеспечение или межсетевой экран.

20. Настройте VipNet/SecretNet для работы в виртуальной среде.

21. Настройте VipNet/SecretNet для работы с различными операционными системами, такими как Windows, Linux, macOS и т.д.

22. Создайте и настройте VPN-туннели для удаленных пользователей, чтобы обеспечить безопасный доступ к ресурсам сети из любой точки мира.

23. Настройте механизмы проверки целостности данных, чтобы обнаруживать и предотвращать любые попытки изменения или подмены данных.

24. Настройте VipNet/SecretNet для работы в различных режимах шифрования, например, AES, DES, RSA и т.д., в зависимости от потребностей вашей сети.

25. Настройте VipNet/SecretNet для автоматического обновления и обновления безопасности, чтобы гарантировать, что ваша сеть всегда защищена от новых угроз и уязвимостей.