МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

УТВЕРЖДАЮ
Директор
НефтИн (филиала) ФГБОУ ВО «ЮГУ»
_____ А.А. Шавырин
«___»_____2022 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

10.02.05
код

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАНЫ СИСТЕМ
(название специальности)

Нижневартовск
-2022-

РАССМОТРЕНО
На заседании ПЦК МиЕНД
Протокол заседания
№ 07 от «31» августа 2022 г.
_____Бойко Я.С.

СОГЛАСОВАНО
Председатель методического совета НефтИн (филиала) ФГБОУ ВО «ЮГУ»
_____Р.И. Хайбулина
«31» августа 2022 г.

Рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем оборудования, разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее - СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем утверждённого приказом Министерства образования и науки РФ от 09.12.2016 г. № 1553.

Организация-разработчик: Нефтяной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Югорский государственный университет»

Разработчики:

Бойко Яна Сергеевна, преподаватель НефтИн (филиала) ФГБОУ ВО «ЮГУ».
Ф.И.О., ученая степень, звание, должность

Согласовано

_____	_____	_____
(подпись, МП)	(инициалы, фамилия)	(занимаемая должность)

Согласовано:

Заведующий библиотекой _____ Л.В. Дементьева

Рецензия
на рабочую программу профессионального модуля
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

для обучающихся очной формы обучения специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем,
разработанную Бойко Яной Сергеевной, преподавателем НефтИн (филиала) ФГБОУ ВО «ЮГУ»

Рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении для обучающихся специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем разработана в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Рабочая программа по данной дисциплине относится к обязательной части основной профессиональной образовательной программы основной профессиональной образовательной программы ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рабочая программа учебной дисциплины ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении состоит из следующих разделов:

1. Общая характеристика рабочей программы учебной дисциплины.
2. Структура и содержание учебной дисциплины.
3. Условия реализации программы учебной дисциплины.
4. Контроль и оценка результатов освоения учебной дисциплины.

Данная программа ориентирована на формирование общей информационной культуры обучающихся и в большей степени связана с мировоззренческими, воспитательными и развивающими задачами в области современных информационных технологий.

В данной программе содержится теоретическая и практическая части, что дает возможность получить разносторонние знания о содержании и сущности информационных технологий и информационных процессов, об архитектуре персонального компьютера и периферийных устройств.

В тематическом плане данной программы предусмотрены лабораторные занятия. Их выполнение позволяет не только приобрести и закрепить навыки работы на компьютере, но и обеспечит возможность проведения промежуточного контроля знаний по практической части дисциплины. Каждый раздел программы отражает тематику и вопросы, позволяющие, в полном объеме, изучить необходимый теоретический материал.

Содержание рабочей программы учебной дисциплины соответствует требованиям Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Рабочая программа содержит минимум литературы, необходимой для изучения данной дисциплины.

Разработанная программа учебной дисциплины рекомендуется для использования в учебном процессе при подготовке обучающихся по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

М.П.

НефтИн (филиал) ФГБОУ ВО «ЮГУ»
методист

(подпись)

Л.Ф. Валиева

РЕЦЕНЗИЯ
на рабочую программу профессионального модуля
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
для обучающихся очной формы обучения специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем,
разработанную Бойко Яной Сергеевной, преподавателем НефтИн (филиала) ФГБОУ ВО «ЮГУ»

Рабочая программа профессионального модуля ***ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении*** для обучающихся специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем разработана в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рекомендуемое количество часов на освоение рабочей программы профессионального модуля разбито на разделы, междисциплинарные курсы и темы.

Программа содержит следующие элементы: титульный лист, паспорт (указана область применения программы, место профессионального модуля в структуре основной образовательной программы, цели и задачи, объем учебной дисциплины и виды учебной работы); тематический план и содержание учебной дисциплины, условия реализации программы (требования к минимальному материально-техническому обеспечению, перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы); контроль и оценка результатов освоения учебной дисциплины.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования на основе Федеральных государственных образовательных стандартов СПО. В паспорте рабочей программы определена область применения рабочей программы, сформулированы цели и задачи, требования к результатам освоения профессионального модуля. - Объем профессионального модуля и виды учебной работы, предусмотренные структурой профессионального модуля, соответствуют тематическому содержанию профессионального модуля. Содержание программы направлено на приобретение обучающимися знаний, умений, направленных на формирование общих и профессиональных компетенций, определенных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и соответствует объему часов, указанному в рабочем учебном плане.

Материально-техническое обеспечение включает наличие учебной лаборатории, оснащенной оборудованием и техническими средствами обучения. Информационное обеспечение обучения содержит перечень современных учебных изданий, дополнительной литературы и интернет-ресурсов. Контроль и оценка результатов освоения профессионального модуля содержит профессиональные и общие, формы, методы контроля оценки результатов обучения и осуществляется преподавателем в процессе проведения различных форм учебных занятий. Рабочая программа позволит студентам в достаточной мере освоить профессиональный модуль, овладеть общими и профессиональными компетенциями, необходимых для качественного освоения программы подготовки специалистов среднего звена.

Заключение: Рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении разработана в полном соответствии с ФГОС СПО и обеспечивает выполнение ФГОС, способствует качественной подготовке специалистов.

Третьяк Б.П., ведущий специалист
по ИТ ООО ЧОП «РН-Охрана»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить основной вид деятельности Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующие ему профессиональные и общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1	**Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 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 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; – администрирования автоматизированных систем в защищенном исполнении;

	– эксплуатации компонентов систем защиты информации автоматизированных систем; – диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении
уметь	– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности
знать	– состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; – принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 801 час, из них
на освоение МДК – 570 часов, в том числе
на промежуточную аттестацию по МДК – 44 часов,
на практики – 182 часа

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	**Объем профессионального модуля, час.**					
			Обучение по МДК, в час.			Практики		Самостоятельная работа[1]
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 1.1. ОК 01– ОК 10	**Раздел 1 модуля.** Установка и настройка автоматизированных (информационных) систем в защищенном исполнении	**262**	**226**	84	–	**36**	–	–
ПК 1.2., ПК 1.3, ПК 1.4 ОК 01– ОК 10	**Раздел 2 модуля.** Администрирование автоматизированных (информационных) систем в защищенном исполнении	**385**	**347**	170	–	**36**	–	*2*
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	**110**					**110**	**–**
	Промежуточная аттестация[2]	**44**	**44**	–	**–**	**–**	**–**	**–**
	Квалификационный экзамен[3]	12	-	–	**–**	**–**	**–**	**–**
	Всего:	**801**	**617**	254	**–**	**72**	**110**	**–**

[1] *Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.*

[2] Выбор формы промежуточной аттестации в основных образовательных программах определяется образовательной организацией.

[3] Часы на экзамен по профессиональному модулю выделяются за счет вариативной части.

2.2. Тематический план и содержание профессионального модуля (ПМ)ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов
1	**2**	**3**
Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении		**276**
МДК.01.01 Операционные системы		**106**
Раздел 1. Элементы теории операционных систем. Свойства операционных систем		
Тема 1.1. Основы теории операционных систем	**Содержание**	**8**
	Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.	8
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	**Содержание**	**18**
	Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.	10
	Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.	
	Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	
	Тематика практических занятий и лабораторных работ	8
	Виртуальные машины. Создание, модификация, работа	
	Установка ОС	
	Создание и изучение структуры разделов жесткого диска	
	Операции с файлами	
Тема 1.3. Модульная структура операционных систем, пространство пользователя	**Содержание**	**8**
	Экзо ядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	4
	Тематика практических занятий и лабораторных работ	4

	Работа в консольном и графическом режимах	
Тема 1.4. Управление памятью	**Содержание**	**8**
	Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти	6
	Тематика практических занятий и лабораторных работ	2
	Мониторинг за использованием памяти	
Тема 1.5. Управление процессами, многопроцессорные системы	**Содержание**	**10**
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие	6
	Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	
	Тематика практических занятий и лабораторных работ	4
	Управление процессами»	
	Наблюдение за использованием ресурсов системы	
Тема 1.6. Виртуализация и облачные технологии	**Содержание**	**8**
	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования	6
	Облачные технологии. Исследования в области виртуализации и облаков	
	Тематика практических занятий и лабораторных работ	2
	Изучение примеров виртуальных машин (VMware, VBox)	
Раздел 2. Безопасность операционных систем		
Тема 2.1. Принципы построения защиты информации в операционных системах	**Содержание**	**12**
	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.	6
	Аутентификация, авторизация, аудит.	
	Тематика практических занятий и лабораторных работ	6
	Управление учетными записями пользователей и доступом к ресурсам	
	Аудит событий системы	
	Изучение штатных средств защиты информации в операционных системах	
Раздел 3. Особенности работы в современных операционных системах		
Тема 3.1. Операционные системы UNIX, Linux,	**Содержание**	**12**
	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux.	8

MacOS и Android	Файловая система UNIX.	
	Операционные системы семейства Mac OS: особенности, преимущества и недостатки.	
	Архитектура Android. Приложения Android	
	Тематика практических занятий и лабораторных работ	4
	Создание дистрибъютиваLinux. Установка.	
	Работа в ОС Linux.	
Тема 3.2. Операционная система Windows	**Содержание**	**8**
	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	6
	Тематика практических занятий и лабораторных работ	2
	Установка и первичная настройка Windows.	
Тема 3.3. Серверные операционные системы	**Содержание**	**10**
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	6
	Тематика практических занятий и лабораторных работ	4
	Работа с сетевой файловой системой.	
	Работа с серверной ОС, например, AltLinux.	
Примерная тематика самостоятельной работы при изучении МДК.01.01 1. Создание виртуальной машины. 2. Установка операционной системы. 3. Анализ журнала аудита ОС на рабочем месте. 4. Изучение аналитических обзоров в области построения систем безопасности операционных систем.		
Промежуточная аттестация по МДК.01.01		**4**
МДК.01.02 Базы данных		**134**
Раздел 1. Основы теории баз данных		
Тема 1.1. Основные понятия теории баз данных. Модели данных	**Содержание**	**6**
	Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования.	6
	Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных.	
	Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	
Тема 1.2. Основы	**Содержание**	**8**

реляционной алгебры	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	4
	Тематика практических занятий и лабораторных работ	4
	Операции над отношениями	
Тема 1.2. Базовые понятия и классификация систем управления базами данных	**Содержание**	**4**
	Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору)	4
Тема 1.3. Целостность данных как ключевое понятие баз данных	**Содержание**	**4**
	Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	4
Раздел 2. Проектирование баз данных		
Тема 2.1. Информационные модели реляционных баз данных	**Содержание**	**6**
	Типы информационных моделей. Логические модели данных. Физические модели данных.	4
	Тематика практических занятий и лабораторных работ	2
	Проектирование инфологической модели данных	
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	**Содержание**	**8**
	Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	4
	Тематика практических занятий и лабораторных работ	4
	Проектирование структуры базы данных	
Тема 2.3. Средства автоматизации проектирования	**Содержание**	**8**
	CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	4
	Тематика практических занятий и лабораторных работ	4
	Проектирование базы данных с использованием CASE-средств	
Раздел 3. Организация баз данных		
Тема 3.1. Создание базы данных. Манипулирование	**Содержание**	**8**
	Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных:	6

данными.	восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	
	Тематика практических занятий и лабораторных работ	2
	Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	**Содержание**	**10**
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	4
	Тематика практических занятий и лабораторных работ	6
	Создание взаимосвязей	
	Сортировка, поиск и фильтрация данных	
	Способы объединения таблиц	
Раздел 4. Управление базой данных с помощью SQL		
Тема 4.1. Структурированный язык запросов SQL	**Содержание**	**6**
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	4
	Тематика практических занятий и лабораторных работ	2
	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	
Тема 4.2. Операторы и функции языка SQL	**Содержание**	**10**
	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	4
	Тематика практических занятий и лабораторных работ	6
	Создание и использование запросов. Группировка и агрегирование данных	
	Коррелированные вложенные запросы	
	Создание в запросах вычисляемых полей. Использование условий	
Раздел 5. Организация распределённых баз данных		
Тема 5.1. Архитектуры распределенных баз данных	**Содержание**	**8**
	Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных.	4
	Отличия и преимущества удаленных баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.	

	Тематика практических занятий и лабораторных работ	2
	Управление доступом к объектам базы данных	
Тема 5.2. Серверная часть распределенной базы данных	**Содержание**	**6**
	Планирование и развёртывание СУБД для работы с клиентскими приложениями	4
	Тематика практических занятий и лабораторных работ	2
	Установка СУБД. Настройка компонентов СУБД.	
Тема 5.3. Клиентская часть распределенной базы данных	**Содержание**	**10**
	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация.	4
	Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа.	
	Оптимизация производительности работы СУБД.	
	Тематика практических занятий и лабораторных работ	6
	Создание форм и отчетов	
	Создание меню. Генерация, запуск.	
	Профилирование запросов клиентских приложений.	
Раздел 6. Администрирование и безопасность		
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	**Содержание**	**6**
	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.	4
	Тематика практических занятий и лабораторных работ	2
	Разработка хранимых процедур и триггеров	
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	**Содержание**	**4**
	Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	4
Тема 6.3. Механизмы защиты информации в системах управления базами данных	**Содержание**	**6**
	Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.	4

	Средства защиты информации в базах данных	

	Тематика практических занятий и лабораторных работ	2
	Управление правами доступа к базам данных	
Тема 6.4. Копирование и перенос данных. Восстановление данных	**Содержание**	**6**
	Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных	4
	Тематика практических занятий и лабораторных работ	4
	Аудит данных с помощью средств СУБД и триггеров	
	Резервное копирование и восстановление баз данных	
Примерная тематика самостоятельной работы при изучении МДК.01.02 1. Выполнение индивидуального задания по теме «Проектирование инфологической модели базы данных». 2. Выполнение индивидуального задания по теме «Нормализация отношений». 3. Подготовка рефератов на тему «Развитие СУБД» (конкретной СУБД). 4. Выполнение индивидуального задания по теме «Создание базы данных. Создание таблиц. Организация межтабличных связей» 5. Выполнение индивидуального задания по теме «Организация запросов». 6. Выполнение индивидуального задания по теме «Создание пользовательского приложения средствами СУБД». 7. Разбор синтаксиса хранимых процедур и триггеров. 8. Подготовка рефератов по теме «Организация и использование механизмов защиты базы данных».		
Промежуточная аттестация по МДК.01.02		**10**
Примерные виды самостоятельных работ при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.		
Учебная практика раздела 1 модуля **Виды работ** 1. Установка программного обеспечения в соответствии с технической документацией. 2. Настройка параметров работы программного обеспечения, включая системы управления базами данных. 3. Настройка компонентов подсистем защиты информации операционных систем. 4. Управление учетными записями пользователей. 5. Работа в операционных системах с соблюдением действующих требований по защите информации. 6. Установка обновления программного обеспечения. 7. Контроль целостность подсистем защиты информации операционных систем. 8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных		**36**

9. Использование программных средств для архивирования информации.		
Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении		**403**
МДК.01.03 Сети и системы передачи информации		**86**
Раздел 1. Теория телекоммуникационных сетей		
Тема 1.1. Основные понятия и определения	**Содержание**	**10**
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	10
Тема 1.2. Принципы передачи информации в сетях и системах связи	**Содержание**	**6**
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	6
Тема 1.3. Типовые каналы передачи и их характеристики	**Содержание**	**14**
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	10
	Тематика практических занятий и лабораторных работ	4
	Расчет пропускной способности канала связи	
Раздел 2. Сети передачи данных		
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	**Содержание**	**30**
	Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи.	8
	Протоколы и интерфейсы управления каналами и сетью передачи данных.	
	Тематика практических занятий и лабораторных работ	22
	Конфигурирование сетевого интерфейса рабочей станции	
	Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	
	Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне	
	Диагностика и разрешение проблем сетевого уровня	
	Диагностика и разрешение проблем протоколов транспортного уровня	
	Диагностика и разрешение проблем протоколов прикладного уровня	
Тема 2.2. Беспроводные системы передачи данных	**Содержание**	**10**
	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	6
	Тематика практических занятий и лабораторных работ	4
	Настройка Wi-Fi маршрутизатора	
Тема 2.3. Сотовые и	**Содержание**	**6**

спутниковые системы	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	6
Примерная тематика самостоятельной работы при изучении МДК.01.03 1. Настройка Wi-Fi маршрутизатора 2. Изучение сетевых утилит 3. Конфигурирование сетевого интерфейса 4. Маршрутизация и управление потоками в сетях связи		
Промежуточная аттестация по МДК.01.03		**10**
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**116**
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		
Тема 1.1. Основы информационных систем как объекта защиты.	**Содержание**	**8**
	Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.	4
	Основные особенности современных проектов АИС. Электронный документооборот.	
	Тематика практических занятий и лабораторных работ	4
	Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	
Тема 1.2. Жизненный цикл автоматизированных систем	**Содержание**	**8**
	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	4
	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	
	Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	
	Тематика практических занятий и лабораторных работ	4
	Разработка технического задания на проектирование автоматизированной системы	
Тема 1.3. Угрозы	**Содержание**	**14**

безопасности информации в автоматизированных системах	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации	2
	Понятие уязвимости угрозы. Классификация уязвимостей.	
	Тематика практических занятий и лабораторных работ	12
	Категорирование информационных ресурсов	
	Анализ угроз безопасности информации	
	Построение модели угроз	
Тема 1.4. Основные меры защиты информации в автоматизированных системах	**Содержание**	**4**
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	4
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	**Содержание**	**10**
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	10
	Ограничение программной среды. Защита машинных носителей информации	
	Регистрация событий безопасности	
	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	
	Обнаружение (предотвращение) вторжений	
	Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации Обеспечение доступности информации	
	Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	
	Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных	
	Резервное копирование и восстановление данных.	
	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	
Тема 1.6. Защита информации в	**Содержание**	**2**
	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура	2

распределенных автоматизированных системах	механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	
Тема 1.7. Особенности разработки информационных систем персональных данных	**Содержание**	**6**
	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	2
	Тематика практических занятий и лабораторных работ	4
	Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	
Раздел 2. Эксплуатация защищенных автоматизированных систем.		
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание**	**4**
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	4
	Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	
	Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	
Тема 2.2. Администрирование автоматизированных систем	**Содержание**	**2**
	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	2
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	**Содержание**	**2**
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	2
Тема 2.4. Защита от несанкционированного доступа к информации	**Содержание**	**6**
	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.	6
	Классификация автоматизированных систем. Требования по защите информации от НСД для АС	
	Требования защищенности СВТ от НСД к информации	
	Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством	

	управления межсетевыми потоками информации, и реализованных в виде МЭ	
Тема 2.5. СЗИ от НСД	**Содержание**	**32**
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.	
	Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.	6
	Обеспечение целостности информационной системы и информации	
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	
	Тематика практических занятий и лабораторных работ	26
	Установка и настройка СЗИ от НСД	
	Защита входа в систему (идентификация и аутентификация пользователей)	
	Разграничение доступа к устройствам	
	Управление доступом	
	Использование принтеров для печати конфиденциальных документов. Контроль печати	
	Настройка системы для задач аудита	
	Настройка контроля целостности и замкнутой программной среды	
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	**Содержание**	**8**
	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	
	Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	
	Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	4
	Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	
	Тематика практических занятий и лабораторных работ	4
	Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	
Тема 2.7. Документация	**Содержание**	**6**

на защищаемую автоматизированную	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на	2

систему	автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	
	Тематика практических занятий и лабораторных работ	4
	Оформление основных эксплуатационных документов на автоматизированную систему.	
Примерная тематика самостоятельной работы при изучении МДК.01.04 1. Разработка концепции защиты автоматизированной (информационной) системы 2. Анализ банка данных угроз безопасности информации 3. Анализ журнала аудита ОС на рабочем месте 4. Построение сводной матрицы угроз автоматизированной (информационной) системы 5. Анализ политик безопасности информационного объекта 6. Изучение аналитических обзоров в области построения систем безопасности 7. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации		
Промежуточная аттестация по МДК.01.04		**4**
МДК.01.05. Эксплуатация компьютерных сетей		**165**
Раздел 1. Основы передачи данных в компьютерных сетях		
Тема 1.1. Модели сетевого взаимодействия	**Содержание**	**6**
	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.	4
	Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	
	Тематика практических занятий и лабораторных работ	2
	Изучение элементов кабельной системы.	
Тема 1.2. Физический уровень модели OSI	**Содержание**	**8**
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.	4
	Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.	
	Оптоволоконные линии связи	
	Стандарты кабелей. Электрическая проводка.	
	Беспроводная среда передачи.	
	Тематика практических занятий и лабораторных работ	4
	Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	
	Сварка оптического волокна	
Тема 1.3. Топология	**Содержание**	**6**
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий**.**	2

компьютерных сетей	**Тематика практических занятий и лабораторных работ**	4
	Разработка топологи сети небольшого предприятия	
	Построение одноранговой сети	
Тема 1.4. Технологии Ethernet	**Содержание**	**6**
	Обзор технологий построения локальных сетей.	4
	Технология Ethernet. Физический уровень.	
	Технология Ethernet. Канальный уровень	
	Тематика практических занятий и лабораторных работ	2
	Изучение адресации канального уровня. MAC-адреса.	
Тема 1.5. Технологии коммутации	**Содержание**	**8**
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.	6
	Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	
	Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети	
	Технология PoweroverEthernet	
	Тематика практических занятий и лабораторных работ	2
	Создание коммутируемой сети	
Тема 1.6. Сетевой протокол IPv4	**Содержание**	**8**
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	6
	Маршрутизация пакетов IPv4	
	Протоколы динамической маршрутизации	
	Тематика практических занятий и лабораторных работ	2
	Изучение IP-адресации.	
Тема 1.7. Скоростные и беспроводные сети	**Содержание**	**4**
	Сеть FDDI. Сеть 100VG-AnyLAN Сверхвысокоскоростные сети Беспроводные сети	2
	Тематика практических занятий и лабораторных работ	2
	Настройка беспроводного сетевого оборудования	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet		
Тема 2.1.	**Содержание**	**6**

Основы коммутации	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов.	4

	Управление потоком в полудуплексном и дуплексном режимах.	
	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	
	Тематика практических занятий и лабораторных работ	2
	Работа с основными командами коммутатора.	
Тема 2.2. Начальная настройка коммутатора	**Содержание**	**8** 4
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.	
	Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.	
	Тематика практических занятий и лабораторных работ	4
	Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	
	Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	
Тема 2.3. Виртуальные локальные сети (VLAN)	**Содержание**	**14** 4
	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.	
	Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation	
	Тематика практических занятий и лабораторных работ	10
	Настройка VLAN на основе стандарта IEEE 802.1Q	
	Настройка протокола GVRP.	
	Настройка сегментации трафика без использования VLAN	
	Настройка функции Q-in-Q (Double VLAN).	
	Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.	
Тема 2.4. Функции повышения надежности и производительности	**Содержание**	**12** 6
	Протокол Spanning Tree Protocol (STP). Уязвимостипротокола STP.	
	Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.	
	Дополнительные функции защиты от петель. Агрегирование каналов связи.	
	Тематика практических занятий и лабораторных работ	6
	Настройка протоколов связующего дерева STP, RSTP, MSTP.	
	Настройка функции защиты от образования петель LoopBackDetection	

	Агрегирование каналов.	
Тема 2.5. Адресация сетевого уровня и маршрутизация	**Содержание**	**20** 6
	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.	
	Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.	
	Планирование подсетей IPv6. Протокол NDP.	
	Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.	
	Тематика практических занятий и лабораторных работ	14
	Основные конфигурации маршрутизатора.	
	Расширенные конфигурации маршрутизатора.	
	Работа с протоколом CDP.	
	Работа с протоколом TELNET. Работа с протоколом TFTP.	
	Работа с протоколом RIP.	
	Работа с протоколом OSPF.	
	Конфигурирование функции маршрутизатора NAT/PAT.	
	Конфигурирование PPP и CHAP.	
Тема 2.6. Качество обслуживания (QoS)	**Содержание**	**6** 4
	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	
	Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.	
	Тематика практических занятий и лабораторных работ	2
	Настройка QoS. Приоритизация трафика. Управление полосой пропускания	
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	**Содержание**	**10** 4
	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.	
	Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.	
	Тематика практических занятий и лабораторных работ	6
	Списки управления доступом (AccessControlList)	
	Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.	
	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	
Тема 2.8. Многоадресная	**Содержание**	**8** 4
	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	

рассылка	Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping). Функция IGMP FastLeave.	
	Тематика практических занятий и лабораторных работ	4
	Отслеживание трафика многоадресной рассылки.	
	Отслеживание трафика Multicast	
Тема 2.9. Функции управления коммутаторами	**Содержание**	**6**
	Управление множеством коммутаторов. Протокол SNMP.	2
	RMON (Remote Monitoring). Функция Port Mirroring.	
	Тематика практических занятий и лабораторных работ	4
	Функции анализа сетевого трафика.	
	Настройка протокола управления топологией сети LLDP.	
Раздел 3. Межсетевые экраны		
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	**Содержание**	**2**
	Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.	2
	Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.	
Тема 3.2. Межсетевые экраны	**Содержание**	**10**
	Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.	2
	Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.	
	Тематика практических занятий и лабораторных работ	8
	Основы администрирования межсетевого экрана	
	Соединение двух локальных сетей межсетевыми экранами	
	Создание политики без проверки состояния.	
	Создание политик для традиционного (или исходящего) NAT.	
	Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing	
Тема 3.3. Системы обнаружения и предотвращения проникновений	**Содержание**	**4**
	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.	2
	Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	
	Тематика практических занятий и лабораторных работ	2
	Обнаружение и предотвращение вторжений.	

Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	**Содержание**	**4**
	Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	2
	Тематика практических занятий и лабораторных работ	2
	Создание альтернативных маршрутов с использованием статической маршрутизации	
Примерная тематика самостоятельной работы при изучении МДК.01.05 1. Физическое кодирование с использованием манчестерского кода 2. Логическое кодирование с использованием скремблирования 3. Подключение клиента к беспроводной сети в инфраструктурном режиме 4. Оценка беспроводной линии связи 5. Проектирования беспроводной сети 6. Сбор информации о клиентских устройствах 7. Планирование производительности и зоны действия беспроводной сети 8. Предпроектное обследование места установки беспроводной сети 9. Обеспечение отказоустойчивости в беспроводных сетях 10. Режимы работы и организация питания точек доступа 11. Сегментация беспроводной сети 12. Настройка QoS 13. Постпроектное обследование и тестирование сети 14. Создание ACL-списка 15. Наблюдение за трафиком в сети VLAN 16. Определение уязвимых мест сети 17. Реализация функций обеспечения безопасности порта коммутатора 18. Исследование трафика 19. Создание структуры сети организации 20. Определение технических требований 21. Мониторинг производительности сети 22. Создание диаграммы логической сети 23. Подготовка к обследованию объекта 24. Обследование зоны беспроводной связи 25. Формулировка общих целей проекта 26. Разработка требований к сети 27. Анализ существующей сети 28. Определение характеристик сетевых приложений		

29. Анализ сетевого трафика 30. Определение приоритетности трафика 31. Изучение качества обслуживания сети 32. Исследование влияния видеотрафика на сеть 33. Определение потоков трафика, построение диаграмм потоков трафика 34. Применение проектных ограничений 35. Определение проектных стратегий для достижения масштабируемости 36. Определение стратегий повышения доступности 37. Определение требований к обеспечению безопасности 38. Разработка ACL-списков для реализации наборов правил межсетевого экрана 39. Использование CIDR для обеспечения объединения маршрутов 40. Определение схемы IP-адресации 41. Определение количества IP-сетей 42. Создание таблицы для выделения адресов 43. Составление схемы сети 44. Анализ плана тестирования и выполнение теста 45. Создание плана тестирования для сети комплекса зданий 46. Проектирование виртуальных частных сетей 47. Безопасная передача данных в беспроводных сетях	
Промежуточная аттестация по МДК.01.05	**4**
Примерные виды самостоятельных работ при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.	**2**
Консультации	**3**
Учебная практика раздела 2 модуля **Виды работ** 1. Проведение аудита защищенности автоматизированной системы. 2. Установка, настройка и эксплуатация сетевых операционных систем. 3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 4. Организация работ с удаленными хранилищами данных и базами данных. 5. Организация защищенной передачи данных в компьютерных сетях. 6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка	***36***

параметров современных сетевых протоколов. 7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. 8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	
Производственная практика **Виды работ:** 1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения 3. Настройка программного обеспечения с соблюдением требований по защите информации 4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам 5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением 6. Настройка встроенных средств защиты информации программного обеспечения 7. Проверка функционирования встроенных средств защиты информации программного обеспечения 8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения 9. Обслуживание средств защиты информации в компьютерных системах и сетях 10. Обслуживание систем защиты информации в автоматизированных системах 11. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем 12. Проверка работоспособности системы защиты информации автоматизированной системы 13. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации 14. Контроль стабильности характеристик системы защиты информации автоматизированной системы 15. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем 16. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	***110***
Экзамен по профессиональному модулю (демонстрационный экзамен)	**12**
Всего	***801***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебного кабинета информатики и лабораторий:

- Информационных технологий, сетей и систем передачи информации, программирования и баз данных;
- Программных и программно-аппаратных средств защиты информации;
- Технических средств защиты информации.

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- посадочные места для обучающихся;
- аудиовизуальный комплекс;
- комплект обучающего материала (комплект презентаций).

Оборудование лаборатории и рабочих мест лаборатории Информационных технологий, сетей и систем передачи информации, программирования и баз данных:

- рабочие места на базе вычислительной техники, подключенными к локальной вычислительной сети и информационно-телекоммуникационной сети "Интернет";
- программным обеспечением сетевого оборудования;
- обучающим программным обеспечением;
- эмуляторами активного сетевого оборудования;
- программным обеспечением межсетевого экранирования и мониторинга технического состояния активного сетевого оборудования.

Оборудование лаборатории и рабочих мест лаборатории Программных и программно-аппаратных средств защиты информации:

- рабочие места на базе вычислительной техники, оснащенные антивирусными программными комплексами;
- программно-аппаратными средствами защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности;
- программными и программно-аппаратными средствами обнаружения вторжений;
- средствами уничтожения остаточной информации в запоминающих устройствах;
- программными средства выявления уязвимостей в автоматизированных системам и средствах вычислительной техники;
- программными средствами криптографической защиты информации; программными средствами защиты среды виртуализации.

Оборудование лаборатории и рабочих мест лаборатории Технических средств защиты информации:

- рабочие места на базе вычислительной техники, оснащенные аппаратными средствами аутентификации пользователя;
- средствами защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;
- средствами измерения параметров физических полей (в том числе электромагнитных излучений и наводок, акустических (виброакустических) колебаний);
- стендами физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов.

3.2. Информационное обеспечение обучения

3.2.1. Печатные и (или) электронные учебные издания (включая учебники и учебные пособия)

1. Батаев А. В. Операционные системы и среды: учебник для студ. учреждений сред. проф. образования / А. В. Батаев, Н. Ю. Налютин, С. В. Синицын – М.: Издательский центр «Академия», 2019 – 272 с.
2. Гостев, И. М. Операционные системы: учебник и практикум для среднего

профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2019. — 164 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

3. Голицына, О. Л. Основы проектирования баз данных: учеб. пособие / О.Л. Голицына, Т.Л. Партыка, И.И. Попов. — 2-е изд., перераб. и доп. — Москва:ФОРУМ: ИНФРА-М, 2019. — 416 с.: ил. — (Среднее профессиональное образование). [Электронный ресурс; Режим доступа http://znanium.com]

4. Гордеев, С. И. Организация баз данных в 2 ч. Часть 1: учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2019. — 310 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

5. Гордеев, С. И. Организация баз данных в 2 ч. Часть 2: учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2019. — 513 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

6. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 1: учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва: Издательство Юрайт, 2019. — 333 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

7. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 2: учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва: Издательство Юрайт, 2019. — 351 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru.

8. Нестеров, С. А. Базы данных: учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва: Издательство Юрайт, 2019. — 230 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

9. Партыка, Т. Л. Операционные системы, среды и оболочки: учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва:ФОРУМ: ИНФРА-М, 2017. — 560 с. : ил. — (Профессиональное образование). [Электронный ресурс; Режим доступа http://znanium.com].

10. 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, 2019. — 363 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

11. Стружкин, Н. П. Базы данных: проектирование: учебник для среднего профессионального образования / Н. П. Стружкин, В. В. Годин. — Москва: Издательство Юрайт, 2019. — 477 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

12. Стружкин, Н. П. Базы данных: проектирование. Практикум: учебное пособие для среднего профессионального образования / Н. П. Стружкин, В. В. Годин. — Москва: Издательство Юрайт, 2019. — 291 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

3.2.2. Методические издания по всем входящим в реализуемые основные образовательные программы учебным предметам, курсам, дисциплинам (модулям) в соответствии с учебным планом:

1. Тен М.Б. МДК.01.01 Операционные системы Методические указания по выполнению практических занятий для обучающихся всех форм обучения образовательных учреждений среднего профессионального обучения специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ) – г. Нижневартовск: ННТ (филиал) ФГБОУ ВО «ЮГУ», 2020 [Электронный ресурс; Режим доступа: Полнотекстовая коллекция учебно-

методических изданий ЮГУ]

3.2.3. Периодические издания:

Теоретический и научно-методический журнал «Среднее профессиональное образование» + Приложение.

3.2.4. Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематикеhttp://depobr.gov35.ru
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» http://www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru

3.3. Адаптация основной образовательной программы обучающимися с ограниченными возможностями здоровья и инвалидов.

Обучение инвалидов и лиц с ограниченными возможностями здоровья по основной образовательной программе осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся. Изучение дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы с обучающимися, в том числе адаптированный сайт филиала, возможностей Интернет-ресурсов, индивидуальных консультаций.

Реализация программы для этой группы обучающихся требует создания безбарьерной среды (обеспечение индивидуально адаптированного рабочего места):

Учебно-методическое обеспечение

При получении образования обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература. Наличия учебно-методического комплекса (учебные программы, учебно-методические пособия, справочники, атласы, тетради на печатной основе, рабочие тетради), фонд оценочных средств (КИМы/КОСы), словари, задания для внеаудиторной самостоятельной работы, презентационные материалы.

Оборудование:

1) для лиц с ограниченными возможностями здоровья по зрению: - наличие альтернативной версии официального сайта филиала в сети «Интернет» для слабовидящих; тактильно-звуковой информатор НОТТ;

2) для лиц с ограниченными возможностями здоровья по слуху: Bluetooth индукционная петля Speak&Go, FM-система Клон;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорнодвигательного аппарата: - материально-технические условия обеспечивают возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения филиала, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных и лестничных проемов, стол рабочий, регулируемый по высоте столешницы, стол для инвалидов-колясочников, регулируемый по высоте с электроприводом и других приспособлений).

При осуществлении образовательного процесса обучающихся с индивидуальными

особенностями (с ограниченными возможностями здоровья) обеспечивается соблюдение следующих общих требований: осуществление образовательной деятельности для обучающихся-инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья.

Все локальные нормативные акты филиала по вопросам организации образовательного процесса по данной образовательной организации доводятся до сведения инвалидов и обучающихся с ограниченными возможностями здоровья в доступной для них форме.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания,	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение

восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

УТВЕРЖДАЮ
Директор
НефтИн (филиала) ФГБОУ ВО «ЮГУ»
_____ А.А. Шавырин
«__» _____2022 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАНЫ СИСТЕМ

10.02.05
код

(название специальности)

Нижневартовск
-2022-

РАССМОТРЕНО
На заседании ПЦК МиЕНД
Протокол заседания
№ 07 от «31» августа 2022 г.
_____Бойко Я.С.

СОГЛАСОВАНО
Председатель методического
совета НефтИн (филиала) ФГБОУ ВО
«ЮГУ»
_____Р.И. Хайбулина
«31» августа 2022 г.

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами, разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее - СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем утверждённого приказом Министерства образования и науки РФ от 09.12.2016 г. № 1553.

Организация-разработчик: Нефтяной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Югорский государственный университет»

Разработчики:

Бойко Яна Сергеевна, преподаватель НефтИн (филиала) ФГБОУ ВО «ЮГУ».
Ф.И.О., ученая степень, звание, должность

Согласовано

_____ _____ _____
(подпись, МП) (инициалы, фамилия) (занимаемая должность)

Согласовано:

Заведующий библиотекой _____ Л.В. Дементьева

Рецензия
на рабочую программу профессионального модуля
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ
для обучающихся очной формы обучения специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем,
разработанную Бойко Яной Сергеевной, преподавателем НефтИн (филиала) ФГБОУ ВО «ЮГУ»

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами для обучающихся специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем разработана в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Рабочая программа по данной дисциплине относится к обязательной части основной профессиональной образовательной программы основной профессиональной образовательной программы ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рабочая программа учебной дисциплины ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами состоит из следующих разделов:

1. Общая характеристика рабочей программы учебной дисциплины.
2. Структура и содержание учебной дисциплины.
3. Условия реализации программы учебной дисциплины.
4. Контроль и оценка результатов освоения учебной дисциплины.

Данная программа ориентирована на формирование общей информационной культуры обучающихся и в большей степени связана с мировоззренческими, воспитательными и развивающими задачами в области современных информационных технологий.

В данной программе содержится теоретическая и практическая части, что дает возможность получить разносторонние знания о содержании и сущности информационных технологий и информационных процессов, об архитектуре персонального компьютера и периферийных устройств.

В тематическом плане данной программы предусмотрены лабораторные занятия. Их выполнение позволяет не только приобрести и закрепить навыки работы на компьютере, но и обеспечит возможность проведения промежуточного контроля знаний по практической части дисциплины. Каждый раздел программы отражает тематику и вопросы, позволяющие, в полном объеме, изучить необходимый теоретический материал.

Содержание рабочей программы учебной дисциплины соответствует требованиям Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Рабочая программа содержит минимум литературы, необходимой для изучения данной дисциплины.

Разработанная программа учебной дисциплины рекомендуется для использования в учебном процессе при подготовке обучающихся по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

М.П.

НефтИн (филиал) ФГБОУ ВО «ЮГУ»
методист _____ Л.Ф. Валиева
(подпись)

РЕЦЕНЗИЯ
на рабочую программу профессионального модуля
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ
для обучающихся очной формы обучения специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем,
разработанную Бойко Яной Сергеевной, преподавателем НефтИн (филиала) ФГБОУ ВО «ЮГУ»

Рабочая программа профессионального модуля ***ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами*** для обучающихся специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем разработана в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

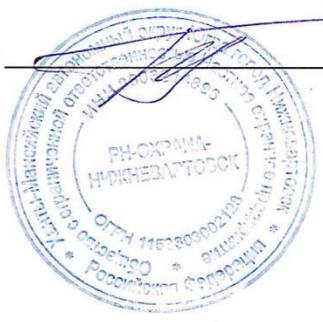
Рекомендуемое количество часов на освоение рабочей программы профессионального модуля разбито на разделы, междисциплинарные курсы и темы.

Выполнение курсового проекта предусмотрено по **МДК.02.01 Программные и программно-аппаратные средства защиты информации** и призвано способствовать формированию профессиональных и общих компетенций у обучающихся. Представленная тематика курсового проектирования актуальна и целесообразна. Она отвечает современным средствам защиты информации.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования на основе Федеральных государственных образовательных стандартов СПО. В паспорте рабочей программы определена область применения рабочей программы, сформулированы цели и задачи, требования к результатам освоения профессионального модуля. - Объем профессионального модуля и виды учебной работы, предусмотренные структурой профессионального модуля, соответствуют тематическому содержанию профессионального модуля. Содержание программы направлено на приобретение обучающимися знаний, умений, направленных на формирование общих и профессиональных компетенций, определенных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и соответствует объему часов, указанному в рабочем учебном плане.

Материально-техническое обеспечение включает наличие учебной лаборатории, оснащенной оборудованием и техническими средствами обучения. Информационное обеспечение обучения содержит перечень современных учебных изданий, дополнительной литературы и интернет-ресурсов. Контроль и оценка результатов освоения профессионального модуля содержит профессиональные и общие, формы, методы контроля оценки результатов обучения и осуществляется преподавателем в процессе проведения различных форм учебных занятий. Рабочая программа позволит студентам в достаточной мере освоить профессиональный модуль, овладеть общими и профессиональными компетенциями, необходимых для качественного освоения программы подготовки специалистов среднего звена.

Заключение: Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана в полном соответствии с ФГОС СПО и обеспечивает выполнение ФГОС, способствует качественной подготовке специалистов.



Третьяк Б.П., ведущий специалист
по ИТ ООО ЧОП «РН-Охрана»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Общие компетенции

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 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 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установки, настройки программных средств защиты информации в автоматизированной системе; обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе.
уметь	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность итестировать функции программно-аппаратных средств защиты информации; применять программные и программно-аппаратные средства для защитыинформации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; применять средства гарантированного уничтожения информации; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
знать	особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.2. Количество часов, отводимое на освоение профессионального модуля
Всего 850 час, из них
на освоение МДК – 524 часов
на практики – 288 часов
на промежуточную аттестацию по ПМ – 28 ч

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Коды профессиональных общих компетенций	Наименования разделов профессиональногомодуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			Всего часов	в том числе		Учебная практик, часов	Производственная практика, часов	
				Лабораторных и практических занятий	Курсовая работа (проект), часов			
ПК 2.1 – ПК 2.6 ОК 01-ОК 10	Раздел 1 модуля. Применение программныхи программно-аппаратных средств защиты информации	156	148	54	30	108	–	–
ПК 2.4 ОК 01-ОК 10	Раздел 2 модуля. Применение криптографических средств защиты информации.	210	202	116	–	36	–	–
ПК 2.1 – ПК 2.3 ОК01-ОК10	Раздел 3 модуля. Применение корпоративной защиты от внутренних угроз информационной безопасности	184	174	104	-	-	-	6
ПК 2.1 – ПК 2.6 ОК 01-ОК10	Учебная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	144						–
ПК 2.1 – ПК 2.6 ОК01-ОК10	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	144					144	
	Промежуточная аттестация	-		–	–	–	–	–
	Квалификационный экзамен	12	-	–	–	–	–	–
	Всего:	850	524	274	30	144	144	-

4Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

5 Выбор формы промежуточной аттестации в основных образовательных программах определяется образовательной организацией самостоятельно.

6 Часы на экзамен по профессиональному модулю выделяются за счет вариативной части.

2.2. Тематический план и содержание профессионального модуля (ПМ) ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		**264**
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**156**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание	2
	Предмет и задачи программно-аппаратной защиты информации	
	Основные понятия программно-аппаратной защиты информации	
	Классификация методов и средств программно-аппаратной защиты информации	
Тема 1.2. Стандарты безопасности	Содержание	2
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	Тематика практических занятий и лабораторных работ	4
	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.	
	Обзор стандартов. Работа с содержанием стандартов	
Тема 1.3. Защищенная автоматизированная система	Содержание	4
	Автоматизация процесса обработки информации	
	Понятие автоматизированной системы	
	Особенности автоматизированных систем в защищенном исполнении.	
	Основные виды АС в защищенном исполнении.	
	Методы создания безопасных систем	

	Методология проектирования гарантированно защищенных КС	
	Дискреционные модели	
	Мандатные модели	
	Тематика практических занятий и лабораторных работ	10
	Учет, обработка, хранение и передача информации в АИС	
	Ограничение доступа на вход в систему.	
	Идентификация и аутентификация пользователей	
	Разграничение доступа	
	Регистрация событий (аудит)	
	Контроль целостности данных	
	Уничтожение остаточной информации	
	Управление политикой безопасности. Шаблоны безопасности	
	Криптографическая защита. Обзор программ шифрования данных	
	Управление политикой безопасности. Шаблоны безопасности	
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	Содержание	2
	Источники дестабилизирующего воздействия на объекты защиты	
	Способы воздействия на информацию	
	Причины и условия дестабилизирующего воздействия на информацию	
	Тематика практических занятий и лабораторных работ	2
	Распределение каналов в соответствии с источниками воздействия на информацию	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание	4
	Понятие несанкционированного доступа к информации	
	Основные подходы к защите информации от НСД	
	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	
	Доступ к данным со стороны процесса	
	Особенности защиты данных от изменения. Шифрование.	
	Тематика практических занятий и лабораторных работ	4
	Организация доступа к файлам	
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	
Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1. Основы защиты автономных	Содержание	4
	Работа автономной АС в защищенном режиме	

автоматизированных систем	Алгоритм загрузки ОС. Штатные средства замыкания среды	
	Расширение BIOS как средство замыкания программной среды	
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	
Тема 2.2. Защита программот изучения	Содержание	4
	Изучение и обратное проектирование ПО	
	Способы изучения ПО: статическое и динамическое изучение	
	Задачи защиты от изучения и способы их решения	
	Защита от отладки	
	Защита от дизассемблирования	
	Защита от трассировки по прерываниям.	
Тема 2.3. Вредоносное программное обеспечение	Содержание	4
	Вредоносное программное обеспечение как особый вид разрушающих воздействий	
	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	
	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	
	Бот-неты. Принцип функционирования. Методы обнаружения	
	Классификация антивирусных средств. Сигнатурный и эвристический анализ	
	Защита от вирусов в "ручном режиме"	
	Основные концепции построения систем антивирусной защиты на предприятии	
	Тематика практических занятий и лабораторных работ	2
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	
Тема 2.4. Защита программи данных от несанкционированного копирования	Содержание	4
	Несанкционированное копирование программ как тип НСД	
	Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	
	Привязка ПО к аппаратному окружению и носителям.	
	Защитные механизмы в современном программном обеспечении на примере MS Office	
	Тематика практических занятий и лабораторных работ	2
	Защита информации от несанкционированного копирования с использованием специализированных программных средств	

	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	
Тема 2.5. Защита информации на машинных носителях	Содержание	4
	Проблема защиты отчуждаемых компонентов ПЭВМ.	
	Методы защиты информации на отчуждаемых носителях. Шифрование.	
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	
	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	
	Безвозвратное удаление данных. Принципы и алгоритмы.	
	Тематика практических занятий и лабораторных работ	6
	Применение средства восстановления остаточной информации на примере Foremost или аналога	
	Применение специализированного программного средства для восстановления удаленных файлов	
	Применение программ для безвозвратного удаления данных	
	Применение программ для шифрования данных на съемных носителях	
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	Содержание	2
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	
	Устройства Touch Memory	
Тема 2.7. Системы обнаружения атак и вторжений	Содержание	4
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	
	Использование сетевых снифферов в качестве СОВ	
	Аппаратный компонент СОВ	
	Программный компонент СОВ	
	Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
	Тематика практических занятий и лабораторных работ	2
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	
Раздел 3. Защита информации в локальных сетях		
Тема 3.1. Основы построения защищенных сетей	Содержание	4
	Сети, работающие по технологии коммутации пакетов	
	Стек протоколов TCP/IP. Особенности маршрутизации.	
	Штатные средства защиты информации стека протоколов TCP/IP.	
	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	

Тема 3.2. Средства организации VPN	Содержание	4
	Виртуальная частная сеть. Функции, назначение, принцип построения	
	Криптографические и некриптографические средства организации VPN	
	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	
	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Тематика практических занятий и лабораторных работ	2
	Развертывание VPN	
Раздел 4. Защита информации в сетях общего доступа		
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	Содержание	4
	Методы защиты информации при работе в сетях общего доступа.	
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности	
	Основные типы firewall. Симметричные и несимметричные firewall.	
	Уровень 1. Пакетные фильтры	
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	
	Уровень 3. Proxy-сервера прикладного уровня	
	Однохостовые и мультихостовые firewall.	
	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций	
	Требования по сертификации межсетевых экранов	
	Тематика практических занятий и лабораторных работ	4
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	
	Изучение различных способов закрытия "опасных" портов	
Раздел 5. Защита информации в базах данных		
Тема 5.1. Защита информации в базах данных	Содержание	4
	Основные типы угроз. Модель нарушителя	
	Средства идентификации и аутентификации. Управление доступом	
	Средства контроля целостности информации в базах данных	
	Средства аудита и контроля безопасности. Критерии защищенности баз данных	
	Применение криптографических средств защиты информации в базах данных	
	Тематика практических занятий и лабораторных работ	4
	Изучение механизмов защиты СУБД MS Access	
	Изучение штатных средств защиты СУБД MSSQL Server	

Раздел 6. Мониторинг систем защиты		
Тема 6.1. Мониторинг систем защиты	Содержание	6
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	
	Классификация отслеживаемых событий. Особенности построения систем мониторинга	
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	
	Классификация сетевых мониторов	
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
	Тематика практических занятий и лабораторных работ	2
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	
	Проведение аудита ЛВС сетевым сканером	
Тема 6.2. Изучение мер защиты информации в информационных системах	Содержание	2
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	
	Тематика практических занятий и лабораторных работ	2
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	
Тема 6.3. Изучение современных программно-аппаратных комплексов.	Тематика практических занятий и лабораторных работ	8
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов	
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	
	Изучение функционала и областей применения DLP систем на примере Info Watch Traffic Monitor или других аналогов	
Курсовая работа		**30**
Примерная тематика курсовых работ		

Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) Проблема защиты информации в облачных хранилищах данных и ЦОДах Защита сред виртуализации	
Примерная тематика самостоятельной работы при изучении МДК.02.01 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	
Промежуточная аттестация по МДК.02.01	8
Примерные виды самостоятельных работ при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.	
Учебная практика по разделу 1 модуля Виды работ: Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности Составление документации по учету, обработке, хранению и передаче конфиденциальной информации Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. Устранение замечаний по результатам проверки Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными	108

средствами, с учетом нормативных правовых актов. Применение математических методов для оценки качества и выбора наилучшего программного средства		
Раздел 2 модуля. Применение криптографических средств защиты информации		**169**
МДК.02.02. Криптографические средства защиты информации		**210**
Введение	Содержание	2
	Предмет и задачи криптографии. История криптографии. Основные термины	
Раздел 1. Математические основы защиты информации		
Тема 1.1. Математические основы криптографии	Содержание	26
	Элементы теории множеств. Группы, кольца, поля.	
	Делимость чисел. Признаки делимости. Простые и составные числа.	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	
	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	Китайская теорема об остатках.	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	Арифметические операции над большими числами.	
	Эллиптические кривые и их приложения в криптографии.	
	Тематика практических занятий и лабораторных работ	14
	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	
	Проверка чисел на простоту	
	Решение задач с элементами теории чисел.	
Раздел 2. Классическая криптография		
Тема 2.1. Методы криптографического защиты информации	Содержание	12
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	
	Методы перестановки. Табличная перестановка, маршрутная перестановка	

	Гаммирование. Гаммирование с конечной и бесконечной гаммами	
	Тематика практических занятий и лабораторных работ	12
	Применение классических шифров замены	
	Применение классических шифров перестановки	
	Применение метода гаммирования	
Тема 2.2. Криптоанализ	Содержание	6
	Основные методы криптоанализа. Криптографические атаки.	
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	
	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Тематика практических занятий и лабораторных работ	18
	Криптоанализ шифра простой замены методом анализа частотности символов	
	Криптоанализ классических шифров методом полного перебора ключей	
	Криптоанализ шифра Вижинера	
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	Содержание учебного материала	10
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	Тематика практических занятий и лабораторных работ	4
	Применение методов генерации ПСЧ	
Раздел 3. Современная криптография		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Содержание учебного материала	6
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	
	Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	
	Тематика практических занятий и лабораторных работ	12
	Кодирование информации	
	Программная реализация классических шифров	
	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	
Тема 3.2. Симметричные системы шифрования	Содержание учебного материала	8
	Общие сведения. Структурная схема симметричных криптографических систем	
	Отечественные алгоритмы Магма и Кузнечик, и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.	

	Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	
	Тематика практических занятий и лабораторных работ	8
	Изучение программной реализации современных симметричных шифров	
Тема 3.3. Асимметричные системы шифрования	Содержание учебного материала	6
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	
	Элементы теории чисел в криптографии с открытым ключом.	
	Тематика практических занятий и лабораторных работ	8
	Применение различных асимметричных алгоритмов.	
	Изучение программной реализации асимметричного алгоритма RSA	
Тема 3.4. Аутентификация данных. Электронная подпись	Содержание учебного материала	6
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Тематика практических занятий и лабораторных работ	12
	Применение различных функций хеширования, анализ особенностей хешей	
	Применение криптографических атак на хеш-функции.	
	Изучение программно-аппаратных средств, реализующих основные функции ЭП	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	Содержание учебного материала	4
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	
	Тематика практических занятий и лабораторных работ	10
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
Тема 3.6. Криптозащита информации в сетях передачи данных	Содержание учебного материала	6
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	
Тема 3.7. Защита информации в электронных платежных системах	Содержание учебного материала	4
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	

	Тематика практических занятий и лабораторных работ	4
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	
Тема 3.8. Компьютерная стеганография	Содержание учебного материала	4
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	Тематика практических занятий и лабораторных работ	8
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	Реализация простейших стеганографических алгоритмов	
Примерная тематика самостоятельной работы при изучении МДК.02.02 История развития криптографии Программная реализация классических шифров Оптимизация методов частотного анализа моноалфавитных шифров. Программная реализация классических шифров Методы механизации шифрования Цифровое представление различных форм информации Анализ современных симметричных криптоалгоритмов Анализ современных асимметричных криптоалгоритмов Программная реализация современных криптоалгоритмов Сравнительный анализ функций хеширования Аутентификация сообщений Законодательство в области криптографической защиты информации Перспективные направления криптографии		
Промежуточная аттестация по МДК.02.02		8
Примерные виды самостоятельной работы при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		
Учебная практика раздела 2 модуля Виды работ: Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи		36
Раздел 3 модуля. Применение корпоративной защиты от внутренних угроз информационной безопасности		**184**

МДК.02.03. Корпоративная защита от внутренних угроз информационной безопасности		**184**
Введение	Содержание	2
	Предмет и задачи корпоративной защиты.	
Раздел 1. Организация работы и управление корпоративной защиты от внутренних угроз информационной безопасности		
Тема 1.1. Организация работы и управление	Содержание	6
	Принципы работы специалиста по информационной безопасности	
	Регламентирующие документы в области информационных систем	
	Скорость изменения ИТ-сферы и области информационной безопасности	
	Тематика практических занятий и лабораторных работ	8
	Организация безопасной, аккуратной и эффективной рабочей зоны	
	Планирование работы специалиста по информационной безопасности в соответствии с изменяющимися приоритетами	
Раздел 2. Установка, конфигурирование и устранение неисправностей		
Тема 2.1. Установка и конфигурирование компонентов DLP системы	Содержание	10
	Сетевое окружение. Сетевые протоколы. Методы выявления и построения путей движения информации в организации. Типы сетевых устройств и их эффективное взаимодействие	
	Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз	
	Процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем	
	Этапы установки системы корпоративной защиты от внутренних угроз	
	Отличия различных версий систем корпоративной защиты от внутренних угроз	
	Тематика практических занятий и лабораторных работ	12
	Конфигурация сетевой инфраструктуры: настройка хост-машины, сетевого окружения, виртуальных машин	
	Установка и настройка системы корпоративной защиты от внутренних угроз	
	Запуск системы, проверка функциональности и соответствия настроек целевой сетевой инфраструктуре	
Тема 2.2. Определение и устранение проблем корпоративной защиты информации	Содержание	8
	Назначение различных компонент версий систем корпоративной защиты от внутренних угроз	
	Технологии программной и аппаратной виртуализации. Особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation	
	Документирования процессов обновления и установки. Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности	

	Популярные аппаратные и программные ошибки	
	Тематика практических занятий и лабораторных работ	14
	Имитация процесса утечки конфиденциальной информации в системе	
	Настройка работоспособности системы и отчет по оценке работоспособности системы	
Раздел 3. Технологии агентского мониторинга		
Тема 3.1. Агентский мониторинг	Содержание	18
	Функции агентского мониторинга	
	Общие настройки системы агентского мониторинга	
	Соединение с LDAP-сервером и синхронизация с Active Directory	
	Политики агентского мониторинга, особенности их настройки	
	Особенности настроек событий агентского мониторинга	
	Механизмы диагностики агента, подходы к защите агента	
	Тематика практических занятий и лабораторных работ	26
	Разработка и применение политики агентского мониторинга для работы с носителями и устройствами	
	Разработка и применение политики агентского мониторинга для работы с файлами	
	Работа с исключениями из перехвата	
Раздел 4. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз		
Тема 4.1. Разработка политики информационной безопасности	Содержание	14
	Технологии работы с политиками информационной безопасности. Создание новых политик, модификация существующих	
	Общие принципы при работе интерфейсом системы защиты корпоративной информации	
	Объекты защиты, персоны	
	Ключевые технологии анализа трафика	
	Типовые протоколы и потоки данных в корпоративной среде. Корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4). Веб-почта	
	Интернет-ресурсы: сайты, блоги, форумы и т. д. (протоколы HTTP, HTTPS). Социальные сети Интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP	
	Принтеры: печать файлов на локальных и сетевых принтерах	
	Тематика практических занятий и лабораторных работ	20
	Разработка политики безопасности, перекрывающей каналы передачи персональных данных сотрудников и контрагентов по электронной почте	
	Разработка политики безопасности, перекрывающей каналы передачи базы клиентов организации в архиве с использованием файловых протоколов	

	Разработка политики безопасности, перекрывающей каналы передачи информации, составляющей коммерческую тайну.	
	Разработка политики безопасности, перекрывающей каналы передачи информации, составляющей коммерческую тайну	
Тема 4.2. Применение политики информационной безопасности	Содержание	12
	Важность полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек. Типы угроз информационной безопасности, типы инцидентов	
	Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации	
	Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации. Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных	
	Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации	
	Роль фильтров при анализе перехваченного трафика. Технические ограничения механизма фильтрации, его преимущества и недостатки	
	Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов	
	Тематика практических занятий и лабораторных работ	24
	Занесение политики информационной безопасности в DLP-систему	
	Модификация объекты защиты, категории, технологии защиты в DLP-системе	
	Применение политики для контроля трафика, выявления и блокирования инцидентов безопасности	
	Интерфейс управления системы корпоративной защиты информации IWTM	
	Механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов	
	Детализированные отчёты о нарушениях	
	Классификацию уровня угрозы инцидента	
Примерная тематика самостоятельной работы при изучении МДК.02.03 История развития корпоративной защиты от внутренних угроз информационной безопасности Виды внутренних угроз информационной безопасности Информационная безопасность в социальных сетях. Информационная безопасность в интернет-мессенджерах		6
Консультации по МДК.02.03		4
Примерные виды самостоятельной работы при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)		

Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	
Производственная практика по ПМ.02 Виды работ – Анализ принципов построения систем информационной защиты производственных подразделений. – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	144
Квалификационный экзамен	**12**
Всего:	**850**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебного кабинета информатики, лаборатории программных и программно-аппаратных средств защиты информации

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя; посадочные места для обучающихся;
- аудиовизуальный комплекс;
- учебно-методический комплекс.

Лаборатория программных и программно-аппаратных средств защиты информации:

-рабочие места студентов, оборудованные персональными компьютерами;

-лабораторные учебные макеты; рабочее место преподавателя;

- учебно-методическое обеспечение модуля;

-интерактивная доска, комплект презентаций;

-антивирусные программные комплексы;

-программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности; программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;

- средства уничтожения остаточной информации в запоминающих устройствах;

- программные средства криптографической защиты информации. Учебно-методический комплекс.

3.2. Информационное обеспечение обучения

3.2.1 Основные печатные и электронные источники:

1. Белов Е. Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования – М.: Издательский центр «Академия», 2017 – 336 с.

2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2019. [Электронный ресурс; Режим доступа http://znanium.com]

3. 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, 2019. — 325 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

3.2.2. Дополнительные источники:

1. Ковалев Д. Р. МДК.02.01 Программные и программно-аппаратные средства защиты информации Методические указания по выполнению практических занятий для обучающихся всех форм обучения образовательных учреждений среднего профессионального обучения специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ) – г. Нижневартовск: ННТ (филиал) ФГБОУ ВО «ЮГУ», 2020 [Электронный ресурс; Режим доступа: Полнотекстовая коллекция учебно-методических изданий ЮГУ]

2. Ковалев Д. Р. МДК.02.02 Криптографические средства защиты информации Методические указания по выполнению практических занятий для обучающихся всех форм обучения образовательных учреждений среднего профессионального обучения специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных

систем» (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ) – г. Нижневартовск: ННТ (филиал) ФГБОУ ВО «ЮГУ», 2020 [Электронный ресурс; Режим доступа: Полнотекстовая коллекция учебно-методических изданий ЮГУ]

3. Ковалев Д. Р. МДК.02.03 Корпоративная защита от внутренних угроз информационной безопасности Методические указания по выполнению практических занятий для обучающихся всех форм обучения образовательных учреждений среднего профессионального обучения специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ) – г. Нижневартовск: ННТ (филиал) ФГБОУ ВО «ЮГУ», 2020 [Электронный ресурс; Режим доступа: Полнотекстовая коллекция учебно-методических изданий ЮГУ]

3.2.3. Периодические издания:

Теоретический и научно-методический журнал «Среднее профессиональное образование» + Приложение

Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.4. Электронные ресурсы:

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

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

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

Справочно-правовая система «Консультант Плюс» www.consultant.ru

Справочно-правовая система «Гарант» www.garant.ru

Федеральный портал «Российское образование www.edu.ru

Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru

Российский биометрический портал www.biometrics.ru

Федеральный портал «Информационно- коммуникационные технологии в образовании» http://www.ict.edu.ru

Сайт Научной электронной библиотеки www.elibrary.ru

3.3. Адаптация основной образовательной программы обучающимися с ограниченными возможностями здоровья и инвалидов.

Обучение инвалидов и лиц с ограниченными возможностями здоровья по основной образовательной программе осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся. Изучение дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы с обучающимися, в том числе адаптированный сайт филиала, возможностей Интернет-ресурсов, индивидуальных консультаций.

Реализация программы для этой группы обучающихся требует создания безбарьерной среды (обеспечение индивидуально адаптированного рабочего места):

Учебно-методическое обеспечение

При получении образования обучающимся с ограниченными возможностями здоровья предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература. Наличия учебно-методического комплекса (учебные программы, учебно-методические пособия, справочники, атласы, тетради на печатной основе, рабочие тетради), фонд оценочных средств (КИМы/КОСы), словари, задания для внеаудиторной самостоятельной работы, презентационные материалы.

Оборудование:

1) для лиц с ограниченными возможностями здоровья по зрению: - наличие альтернативной версии официального сайта филиала в сети «Интернет» для слабовидящих; тактильно-звуковой информатор НОТТ;

2) для лиц с ограниченными возможностями здоровья по слуху: Bluetooth индукционная петля Speak&Go, FM-система Клон;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: - материально-технические условия обеспечивают возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения филиала, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных и лестничных проемов, стол рабочий, регулируемый по высоте столешницы, стол для инвалидов-колясочников, регулируемый по высоте с электроприводом и других приспособлений).

При осуществлении образовательного процесса обучающихся с индивидуальными особенностями (с ограниченными возможностями здоровья) обеспечивается соблюдение следующих общих требований: осуществление образовательной деятельности для обучающихся-инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья.

Все локальные нормативные акты филиала по вопросам организации образовательного процесса по данной образовательной организации доводятся до сведения инвалидов и обучающихся с ограниченными возможностями здоровья в доступной для них форме.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации.	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных

		задач, оценка процесса и результатов выполнения видов работ напрактике.
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации.	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике.
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике.
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств.	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике.
ПК2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике.
ОК 01. Выбирать способы	- обоснованность постановки	Интерпретация результатов

решения задач профессиональной деятельности, применительно различным контекстам.	цели,выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач.	наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам. Экзамен квалификационный.
ОП 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.	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	-демонстрация ответственности за принятыерешения; -обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных).	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- грамотность устной и письменной речи; - ясность формулирования и изложения мыслей.	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик.	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению,	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной	

эффективно действовать вчрезвычайных ситуациях.	практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций.	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	-эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

УТВЕРЖДАЮ
Директор
НефтИн (филиала) ФГБОУ ВО «ЮГУ»
_____ А.А. Шавырин
«31» августа 2022 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ
индекс (название дисциплины)

10.02.05 Обеспечение информационной безопасности автоматизированных систем
код (название специальности)

НИЖНЕВАРТОВСК
-2022-

РАССМОТРЕНО
На заседании ПЦК ЭТД
Протокол заседания
№ 7 от «31» августа 2022г.
_____Тен М.Б.

СОГЛАСОВАНО
Председатель Методического совета НефтИн (филиала) ФГБОУ ВО «ЮГУ»
_____Хайбуллина Р.И.
«31» августа 2022г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Организация-разработчик: Нефтяной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Югорский государственный университет»

Разработчики:

Давиденко Ирина Викторовна - преподаватель НефтИн (филиала) ФГБОУ ВО «ЮГУ»
Ф.И.О., ученая степень, звание, должность

Даценко Оксана Владимировна - преподаватель НефтИн (филиала) ФГБОУ ВО «ЮГУ»
Ф.И.О., ученая степень, звание, должность

Согласовано:

Заведующий библиотекой _____ Л.В. Дементьева

Рецензенты:

1.Внутренний рецензент

Тен Марина Борисовна	Преподаватель вышей категории	НефтИн (филиал) ФГБОУ ВО «ЮГУ»

2. Внешний рецензент

Даценко Евгений Сергеевич	Начальник ПТО	Нижневартовский филиал ООО «РН-Бурение»

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля

ПМ.03 Защита информации техническими средствами

для обучающихся по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

преподавателя НефтИн (филиала) ФГБОУ ВО «ЮГУ»

Даценко Оксаны Владимировны

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана в соответствии с требованиями ФГОС СПО и учебным планом по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Рабочая программа по профессиональному модулю относится к обязательной части программы подготовки специалистов среднего звена СПО по специальности 10.02.05.

Рабочая программа включает в себя следующие элементы: паспорт рабочей программы профессионального модуля; результаты освоения профессионального модуля, структуру и содержание профессионального модуля; условия реализации профессионального модуля; контроль и оценка результатов освоения профессионального модуля (вида профессиональной деятельности)

В паспорте программы сформулированы область применения рабочей программы, цели и задачи освоения профессионального модуля, направленные на приобретение практического опыта и овладение обучающимися общими и профессиональными компетенциями.

Тематический план имеет оптимальное распределение часов по разделам и темам в соответствии с учебным планом специальности 10.02.05.

Каждый раздел программы отражает тематику и вопросы, позволяющие, в полном объеме, изучить необходимый теоретический материал. Проведение практических занятий, предусмотренных рабочей программой, позволяют приобрести необходимые навыки, сформировать профессиональные компетенции.

Рабочая программа содержит перечень литературы, необходимой для изучения профессионального модуля.

В целом разработанная рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами актуальна, соответствует требованиям программы подготовки специалистов среднего звена Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и рекомендуется для использования в учебном процессе при подготовке обучающихся по этой специальности.

Рецензент

_____ Тен М.Б., преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ»

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля
ПМ.03 Защита информации техническими средствами
для обучающихся 10.02.05 Обеспечение информационной безопасности автоматизированных систем

направления подготовки (специальности)
разработана преподавателями НефтИн (филиала) ФГБОУ ВО «ЮГУ»:
Даценко Оксаной Владимировной, Давиденко Ириной Викторовной

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами обучающихся направления программы подготовки специалистов среднего звена (ППССЗ) специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем разработана в соответствии с требованиями ФГОС СПО

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана в соответствии с приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и примерной программой профессионального модуля ПМ.03 Защита информации техническими средствами профессиональных образовательных организаций, реализующих основную профессиональную образовательную программу СПО на базе основного общего образования с одновременным получением среднего общего образования.

Рабочая программа составлена логично. Последовательность разделов и тем, предлагаемых к изучению, направлена на качественное усвоение учебного материала. Содержание рабочей программы соответствует минимуму содержания, который установлен образовательным стандартом.

Представленная рабочая программа обеспечивает выполнение Федерального государственного образовательного стандарта, способствует качественной подготовке обучающихся среднего специального образования.

Нижневартовский филиал ООО «РН-Бурение» Даценко Евгений Сергеевич

(подпись)

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации техническими средствами* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	**Защита информации техническими средствами**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 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 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.
уметь	– применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации
знать	– порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты

	информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 727 час, из них

на освоение МДК – 444 час, в том числе

на промежуточную аттестацию по МДК – 28 часов,

на практики – 255 часа

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.03 Защита информации техническими средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 3.1-ПК.3.4 ОК 01–ОК10	**Раздел 1 модуля.** Применение технической защиты информации	**252**	**180**	102	–	**72**	–	–
ПК 3.5 ОК 01–ОК10	**Раздел 2 модуля.** Применение инженерно-технических средств физической защиты объектов информатизации	**300**	**264**	126	30	**36**	–	–
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	**147**					**147**	–
	Промежуточная аттестация	**16**	**16**	–	**–**	**–**	**–**	**–**
	Квалификационный экзамен	**12**		–	**–**	**–**	**–**	**–**
	Всего:	**727**	**444**	228	30	**108**	**147**	–

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение технической защиты информации		**252**
МДК.03.01 Техническая защита информации		**180**
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**4**
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**4**
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	**Содержание**	**6**
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Тематика практических занятий и лабораторных работ	**6**
	Изучение основных руководящих, нормативных и методических документов по защите информации	
Тема 2.2. Технические	**Содержание**	**4**

каналы утечки информации	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Тематика практических занятий и лабораторных работ	**6**
	Угрозы информационной безопасности	
Тема 2.3. Методы и средства технической разведки	**Содержание**	**4**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика практических занятий и лабораторных работ	**6**
	Организация аттестации выделенного помещения по требованиям безопасности информации	
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**6**
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практических занятий и лабораторных работ	**6**
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**6**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Тематика практических занятий и лабораторных работ	**6**
	Защита аппаратуры от электромагнитных полей	
Раздел 4. Системы защиты от утечки информации		
Тема 4.1. Системы за-	**Содержание**	**4**

щиты от утечки информации по акустическому каналу	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	
	Тематика практических занятий и лабораторных работ	**6**
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**4**
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Тематика практических занятий и лабораторных работ	**6**
	Системы защиты от утечки информации по проводному каналу	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**4**
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Тематика практических занятий и лабораторных работ	**6**
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**4**
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	
	Тематика практических занятий и лабораторных работ	**12**
	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	

Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**4**
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Тематика практических занятий и лабораторных работ	**6**
	Технические средства защиты информации в телефонных линиях	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**4**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Тематика практических занятий и лабораторных работ	**6**
	Системы защиты от утечки информации по электросетевому каналу	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**4**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Тематика практических занятий и лабораторных работ	**6**
	Системы защиты от утечки информации по оптическому каналу	
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**8**
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
	Тематика практических занятий и лабораторных работ	**12**
	Применение технических средств защиты информации	

Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**8**
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Тематика практических занятий и лабораторных работ	**12**
	Эксплуатация технических средств защиты информации	
Промежуточная аттестация по МДК.03.01		**8**
Примерные виды самостоятельной работы при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		
Учебная практика **Виды работ:** – Измерение параметров физических полей. – Определение каналов утечки ПЭМИН. – Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. – Установка и настройка технических средств защиты информации. – Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации.		**72**
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		**300**
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**180**
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты объектов информатиза-	**Содержание**	**8**
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Кате-	

ции	горирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	
	Тематика практических занятий и лабораторных работ	**6**
	Характеристика объекта защиты	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**8**
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Тематика практических занятий и лабораторных работ	**10**
	Анализ нормативно-правовой базы физической защиты. Формирование требований к физической защите объекта	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**10**
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Тематика практических занятий и лабораторных работ	**10**
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**12**
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	

	Тематика практических занятий и лабораторных работ	**6**
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**10**
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
	Тематика практических занятий и лабораторных работ	**6**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**8**
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	
	Тематика практических занятий и лабораторных работ	**6**
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5 Система воздействия	**Содержание**	**6**
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Тематика практических занятий и лабораторных работ	**6**
	Выбор и обоснование средств подсистемы задержки	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание**	**8**
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	

	Тематика практических занятий и лабораторных работ	**10**
	Разработка структурной схемы и спецификации оборудования	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**8**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	
	Тематика практических занятий и лабораторных работ	**12**
	Эксплуатация инженерно- технических средств физической защиты	
Курсовой проект		**30**
Примерная тематика курсового проекта 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.		
Примерная тематика самостоятельной работы при изучении МДК.03.02 – Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. – Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты.		
Промежуточная аттестация по МДК.03.02		**8**
МДК.03.03 Физические основы защиты информации / Основы интеллектуального труда		**84**
Раздел 1. Обеспечение информационной безопасности		
Тема1.1 Правовое обеспечение информационной безопасности	**Содержание**	**4**
	Информационное право в теории государства и права. Информация как объект правового регулирования. Защита информации. Информация ограниченного доступа. Лицензирование деятельности в области защиты информации. Сертификация, стандартизация, аккредитация в информационной сфере. Шифровальные (криптографические) средства защиты информации. Электронная цифровая подпись (ЭЦП). Юридическая ответственность за нарушение норм защиты информации	

	Тематика практических занятий и лабораторных работ	**10**
	Применение правовых основ использования организационных и технических средств защиты информации.	
Тема1.2 Организационное обеспечение информационной безопасности	**Содержание**	**4**
	Функции организационной составляющей системы защиты информации. Регламентация работы с информацией и её носителями. Регламентация действий при осуществлении информационных процессов. Регламентация работы с элементами системы защиты информации	
Раздел 2. Информационная безопасность в различных системах		
Тема 2.1 Безопасность операционных систем	**Содержание**	**2**
	Ресурсы операционной системы. Методы обеспечения информационной безопасности в операционных системах.	
	Тематика практических занятий и лабораторных работ	**10**
	1.Применение различных методов обеспечения информационной безопасности в операционных системах 2.Аутентификация в операционных системах. 3.Разграничение доступа к защищаемым объектам. 4.Аудит событий.	
Тема 2.2 Безопасность систем баз данных	**Содержание**	**4**
	Ведение в базы данных. Безопасность баз данных.	
Тема 2.3 Безопасность вычислительных систем	**Содержание**	**6**
	Основные термины и определения. Классификация сетей. Типовая сеть крупной организации. Уровни информационной инфраструктуры корпоративной сети. Классификация угроз, уязвимостей, атак. Защитные механизмы и контрмеры.	
	Тематика практических занятий и лабораторных работ	**10**
	Применение защитных мер безопасности вычислительных систем в корпоративной сети	
Раздел 3. Методы защиты информации		
Тема 3.1 Криптогра-	**Содержание**	**6**

фические методы защиты информации	Терминология. Угрозы со стороны участников информационного обмена. Требования к криптосистемам. Симметричные криптосистемы. Криптографические хэш-функции. Ассиметричные криптосистемы (криптосистемы с открытым ключом). Характеристики безопасности обеспечиваемые средствами криптографической защиты информации. Удостоверяющий центр.	
	Тематика практических занятий и лабораторных работ	**24**
	1.Основные алгоритмы шифрования 2.Криптоанализ и атаки на криптосистемы 3.Управление ключами	
Тема 3.2 Технические каналы утечки информации	**Содержание**	**4**
	Общие понятия. Технические каналы утечки информации. Структура, классификация и основные характеристики.	
Примерные виды самостоятельной работы при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите. Работа над курсовым проектом: планирование выполнения курсового проекта, определение задач работы, изучение литературных источников, проведение предпроектного исследования.		
Учебная практика по разделу 2 модуля 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления.		***36***

8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации.	
Производственная практика профессионального модуля **Виды работ** 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	***147***
Квалификационный экзамен	***12***
Всего	***727***

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

лекционные аудитории с мультимедийным оборудованием; лаборатория «Технических средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест – не менее 30, рабочее место преподавателя, проектор, персональный компьютер, интерактивная доска, комплект презентаций.

Оборудование лаборатории «Технических средств защиты информации» и рабочих мест лаборатории:

1) рабочие места студентов, оборудованные персональными компьютерами;
2) лабораторные учебные макеты;
3) аппаратные средства аутентификации пользователя;
4) средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;
5) средства измерения параметров физических полей;
6) стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
7) рабочее место преподавателя;
8) учебно-методическое обеспечение модуля;
9) интерактивная доска, комплект презентаций.

3.2. Информационное обеспечение обучения

3.2.1. Печатные и (или) электронные учебные издания (включая учебники и учебные пособия):

1. Белов Е. Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования – М.: Издательский центр «Академия», 2017 – 336 с.
2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва :ИЦ РИОР, НИЦ ИНФРА-М, 2019. [Электронный ресурс; Режим доступа http://znanium.com]
3. 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, 2022. — 325 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

3.2.3. Печатные издания:

1. Теоретический и научно-методический журнал «Среднее профессиональное образование» + Приложение

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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 Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОП 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	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодей-	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обуче-	

ствовать с коллегами, руководством, клиентами.	ния, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)

НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

УТВЕРЖДАЮ
Директор НефтИн
(филиала) ФГБОУ ВО «ЮГУ»
_____ А.А. Шавырин
«31» августа 2022 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ
индекс (название дисциплины)

ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН

10.02.05 Обеспечение информационной безопасности автоматизированных систем
код (название специальности)

НИЖНЕВАРТОВСК
-2022-

РАССМОТРЕНО
На заседании ПЦК ЭТД
Протокол заседания
№ 7 от «31» августа 2022г.
_____Тен М.Б.

СОГЛАСОВАНО
Председатель Методического совета НефтИн (филиала) ФГБОУ ВО «ЮГУ»
_____ Хайбулина Р.И.
«31» августа 2022г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Организация-разработчик: Нефтяной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Югорский государственный университет»

Разработчики:

Тен М.Б., высшая категория, преподаватель
Ф.И.О., ученая степень, звание, должность

Согласовано:

Заведующий библиотекой _____ Л.В. Дементьева

Рецензенты:

1.Хакимова И.В., высшая категория, преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ»

2. Третяк Б.П., ведущий специалист по ИТ ООО ЧОП «РГ-Охрана»

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин

для обучающихся по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

преподавателя НефтИн (филиала) ФГБОУ ВО «ЮГУ»

Тен Марины Борисовны

Рабочая программа профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин разработана в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Рабочая программа по профессиональному модулю относится к обязательной части программы подготовки специалистов среднего звена СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа включает в себя следующие элементы:

- паспорт рабочей программы профессионального модуля;
- результаты освоения профессионального модуля, структуру и содержание профессионального модуля;
- условия реализации профессионального модуля;
- контроль и оценка результатов освоения профессионального модуля (вида профессиональной деятельности)

В паспорте программы сформулированы область применения рабочей программы, цели и задачи освоения профессионального модуля, направленные на приобретение практического опыта и овладение обучающимися общими и профессиональными компетенциями необходимыми по профессии 16199 Оператор электронно-вычислительных и вычислительных машин.

Тематический план имеет оптимальное распределение часов по разделам и темам в соответствии с учебным планом специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Все разделы программы отражают тематику и вопросы, позволяющие изучить необходимый теоретический материал. Проведение практических занятий, предусмотренных рабочей программой, позволяют приобрести необходимые навыки, сформировать профессиональные компетенции.

В целом разработанная рабочая программа профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин актуальна, соответствует требованиям программы подготовки специалистов среднего звена Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и рекомендуется для использования в учебном процессе при подготовке обучающихся по этой специальности.

Рецензент _____ И.В. Хакимова, преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ»

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин

для обучающихся по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем
преподавателя НефтИн (филиала) ФГБОУ ВО «ЮГУ»
Тен Марины Борисовны

Рабочая программа профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин разработана в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем Рабочая программа по профессиональному модулю относится к обязательной части программы подготовки специалистов среднего звена СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа включает в себя следующие элементы: паспорт рабочей программы профессионального модуля; результаты освоения профессионального модуля, структуру и содержание профессионального модуля; условия реализации профессионального модуля; контроль и оценка результатов освоения профессионального модуля (вида профессиональной деятельности)

В паспорте программы сформулированы область применения рабочей программы, цели и задачи освоения профессионального модуля, направленные на приобретение практического опыта и овладение обучающимися общими и профессиональными компетенциями.

Тематический план имеет оптимальное распределение часов по разделам и темам в соответствии с учебным планом специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Каждый раздел программы отражает тематику и вопросы, позволяющие, в полном объеме, изучить необходимый теоретический материал. Проведение практических занятий, предусмотренных рабочей программой, позволяют приобрести необходимые навыки, сформировать профессиональные компетенции.

Рабочая программа содержит перечень литературы, необходимой для изучения профессионального модуля.

В целом разработанная рабочая программа профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин актуальна, соответствует требованиям программы подготовки специалистов среднего звена Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и рекомендуется для использования в учебном процессе при подготовке обучающихся по этой специальности.

Рецензент

_____ Б.П. Третяк, ведущий специалист по ИТ ООО ЧОП «РН-Охрана»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 4	**Выполнять работы по профессии «Оператор электронно-вычислительных и вычислительных машин»**
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 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 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь	− выполнения требований техники безопасности при работе с

практический опыт	вычислительной техникой; – организации рабочего места оператора электронно-вычислительных и вычислительных машин; – подготовки оборудования компьютерной системы к работе; – инсталяции, настройки и обслуживания программного обеспечения компьютерной системы; – управления файлами; – применения офисного программного обеспечения в соответствии с прикладной задачей; – использования ресурсов локальной вычислительной сети; – использования ресурсов, технологий и сервисов Интернет; – применения средств защиты информации в компьютерной системе.
уметь	– выполнять требования техники безопасности при работе с вычислительной техникой; – производить подключение блоков персонального компьютера и периферийных устройств; – производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; – диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; – выполнять инсталляцию системного и прикладного программного обеспечения; – создавать и управлять содержимым документов с помощью текстовых процессоров; – создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; – создавать и управлять содержимым презентаций с помощью редакторов презентаций; – использовать мультимедиа проектор для демонстрации презентаций; – вводить, редактировать и удалять записи в базе данных; – эффективно пользоваться запросами базы данных; – создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; – производить сканирование документов и их распознавание; – производить распечатку, копирование и тиражирование документов на принтере и других устройствах; – управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; – осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; – осуществлять поиск, сортировку и анализ

	информации с помощью поисковых интернет сайтов; – осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; – осуществлять резервное копирование и восстановление данных.
знать	– требования техники безопасности при работе с вычислительной техникой; – основные принципы устройства и работы компьютерных систем и периферийных устройств; – классификацию и назначение компьютерных сетей; – виды носителей информации; – программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета; – основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 204 часа, из них

на МДК – 48 часов

на практики – 144 часа

промежуточная аттестация – 12 часов

2. СТРУКТУРА И СОДЕЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа[1]
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 4.1 – ПК 4.4 ОК1–ОК 10	**Раздел 1 модуля**. Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»	**120**	48	28	–	72	–	–
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	**72**					72	–
	Промежуточная аттестация[2]		**-**	–	**–**	**–**	**–**	**–**
	Квалификационный экзамен[3]	**12**	**-**	–	**–**	**–**	**–**	**–**
	Всего:	**204**	**-**	–	–	72	72	–

2.2. *Тематический план и содержание профессионального модуля (ПМ)*

[1]Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

[2] Выбор формы промежуточной аттестации в основных образовательных программах определяется образовательной организацией самостоятельно.

[3] Часы на экзамен по профессиональному модулю выделяются за счет вариативной части.

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся	Объем часов
1	**2**	**3**
Раздел модуля 1. Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»		**120**
МДК.04.01 Выполнение работ по рабочей профессии		**48**
Раздел 1. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных		
Тема 1.1. Работа в текстовом процессоре	**Содержание**	**14**
	Сканирование текстовых документов и их распознавание Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов Форматирование и редактирование документов в текстовом процессоре.	6
	Тематика практических занятий и лабораторных работ	8
	Работа с таблицами в текстовом процессоре.	
	Работа с диаграммами в текстовом процессоре.	
	Работа с графическими объектами в текстовом процессоре.	
	Печать документов в текстовом процессоре.	
Тема 1.2. Работа в редакторе электронных таблиц	**Содержание**	**14**
	Создание и форматирование таблицы в редакторе электронных таблиц Вычисление с помощью формул в электронной таблице Работа со встроенными функциями в электронной таблице	6
	Тематика практических занятий и лабораторных работ	8
	Работа со списками в электронной таблице	
	Создание форм для ввода данных в таблицы	
	Создание и работа с диаграммами и графиками	

	Обмен данными между текстовым процессором и электронной таблицей	
Тема 1.3. Работа в программе подготовки и просмотра презентаций	**Содержание**	**10**
	Построение презентации различными способами Обработка объектов слайдов презентации.	4
	Тематика практических занятий и лабораторных работ	6
	Настройка анимации объектов	
	Настройка показа и демонстрация результатов работы средствами мультимедиа	
Тема 1.4. Работа в системе управления базами данных	**Содержание**	**10**
	Основные понятия о базах данных. Ввод данных в таблицы базы данных	4
	Тематика практических занятий и лабораторных работ	6
	Создание простых запросов без параметров	
	Создание запросов с параметрами	
	Создание отчетов	
Примерная тематика самостоятельной работы при изучении МДК.04.01 Форматирование электронных таблиц разного уровня сложности. Расчет данных электронных таблиц с использованием формул. Создание связанных таблиц на нескольких листах. Создание и оформление слайдов с использованием текстовой, графической и мультимедийной информации. Работа со сканером. Установка драйвера устройства, программы для работы со сканером. Настройка и оптимизация компьютера Установка программного обеспечения Распечатка документов на принтере и плоттере Настройка локальной сети Создание электронных тестов Антивирусная защита своего рабочего места		
Промежуточная аттестация по МДК.04.01		**-**
УП.04.01 Учебная практика		**72**
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения		**24**
Тема 1.1.	**Тематика практических занятий и лабораторных работ**	**8**

Работа с устройствами компьютерной системы	Соблюдение техники безопасности при работе на ЭВМ Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка Установка и замена расходных материалов для принтеров, ксерокса, плоттера.	
Тема 1.2. Работа с программным обеспечением компьютерной системы	**Тематика практических занятий и лабораторных работ**	**8**
	Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети). Установка прикладных программ. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете	
Тема 1.3. Диагностика неисправностей системы, ведение документации	**Тематика практических занятий и лабораторных работ**	**8**
	Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ	
Раздел 2. Работа в графических редакторах		**30**
Тема 2.1. Работа в графических редакторах	**Тематика практических занятий и лабораторных работ**	**30**
	Рисование объектов средствами графического редактора. Работа с заливками и контурами в программе векторной графики. Работа с текстом в программе векторной графики. Работа с эффектами программе векторной графики. Вставка и редактирование готового изображения с использованием программ растровой графики. Работа с цветом с использованием программ растрой графики. Работа со слоями с использованием программ растрой графики. Работа со спецэффектами с использованием программ растровой графики.	
Раздел 3. Использование ресурсов технологий и сервисов Интернета		**8**
Тема 3.1. Работа с ресурсами Интернета	**Тематика практических занятий и лабораторных работ**	**8**
	Создание и обмен письмами электронной почты. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера.	

	Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов. Пересылка и публикация файлов данных в Интернете.	
Раздел 4. Обеспечение защиты информации в компьютерной системе		**10**
Тема 4.1. Защита информации при работе с офисными приложениями	**Тематика практических занятий и лабораторных работ**	**10**
	Использование штатных средств защиты операционной системы и прикладных программ. Применение парольной защиты. Установка антивирусных программ, их настройка. Обновление базы. Выполнение архивирования данных. Выполнение резервного копирования и восстановления данных	
Промежуточная аттестация по учебной практике		**-**
Производственная практика **Виды работ:** 1. Установка офисного программного обеспечения 2. Приобретение навыков работы в текстовом редакторе Microsoft Word - подключение основных панелей инструментов, их настройка, описание и назначение - форматирование текстовых, табличных, графических и смешанных документов - передача информации в другие программы - получение информации из внешних источников - создание гиперссылок - подготовка и распечатка документов на принтере и плоттере 3. Приобретение навыков работы в табличном процессоре EXCEL 4. Приобретение навыков работы в Microsoft PowerPoint. 5. ABBYY FineReader. Настройка интерфейса, режимов сканирования, сохранение во внешнее приложение 6. Сканирование и обработка текстовых документов 7. Сканирование и обработка таблиц и графических изображений 8. Работа с папками и файлами (создание, копирование, перемещение, удаление, переименование). Способы просмотра информации. Работа с проводником файлов. 9. Установка и настройка принтера с помощью внутренних и внешних драйверов. Настройка экрана, клавиатуры, мыши. 10.Оптимизация операционной системы. Восстановление системы. 11.Способы запуска приложений и прикладных программ. Ярлыки. Поиск информации на локальных носителях и локальной сети. 12.Оптимизация работы приложений.		***72***

13.Определение установленного оборудования с помощью сервисных программ. Диагностика неполадок. Модернизация оборудования. 14.Установка и удаление основных и дополнительных пакетов прикладных программ 15.Работа с архиваторами ZIP и RAR. Создание, распаковка, просмотр, удаление архивных файлов 16.Работа с антивирусными программами. Тестирование, лечение дисков, флешек, карт памяти 17.Приобретение опыта по заправке бумаги в принтеры, установке картриджей различного типа, красящих лент, устранению аварийных ситуаций. 18.Приобретение опыта по обслуживанию очереди вывода на печать в WINDOWS, удаление из очереди ненужных файлов. 19.Настройка сетевого принтера 20.Знакомство с технологией и графиком работы получения и рассылки электронной почты по каналам INTERNET в данном структурном подразделении 21. Ознакомление с техникой подключения к Интернет, запуска программы электронной почты, поиска и просмотра информации, копирование и сохранения нужных файлов, отправки информации по требуемому адресу	
Экзамен по профессиональному модулю	**12**
Всего	**204**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы модуля предполагает наличие лаборатории информационных технологий, сетей и систем передачи информации, программирования и баз данных.

Оборудование лаборатории информационных технологий:

Компьютеры, подключенными к локальной вычислительной сети и информационно-телекоммуникационной сети "Интернет", проектор, экран, акустическая система.

Программное обеспечение: (операционные системы, пакет прикладных программ, графические редакторы, справочная правовая система, браузер, антивирусная программа)

Учебно-наглядные пособия: схемы, таблицы, учебные презентации

Раздаточный дидактический материал: учебные карточки с заданиями, дидактический материал для выполнения практических работ.

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные и электронные источники:

1. Колдаев, В. Д. Архитектура ЭВМ : учебное пособие / В.Д. Колдаев, С.А. Лупин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2020. — 383 с. — (Среднее профессиональное образование). [Электронный ресурс; Режим доступа http://znanium.com
2. Новожилов, О. П. Архитектура компьютерных систем в 2 ч. Часть 1 : учебное пособие для среднего профессионального образования / О. П. Новожилов. — Москва : Издательство Юрайт, 2019. — 276 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]
3. Новожилов, О. П. Архитектура компьютерных систем в 2 ч. Часть 2 : учебное пособие для среднего профессионального образования / О. П. Новожилов. — Москва : Издательство Юрайт, 2019. — 246 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]
4. Струмпэ Н. В. Оператор ЭВМ Практические работы: учеб. пособие для студ. учреждений сред. проф. образования – М.: Издательский центр «Академия», 2018 – 112 с.

3.2.2. Дополнительные печатные источники:

1. Теоретический и научно-методический журнал «Среднее профессиональное образование» + Приложение

3.2.3. Электронные источники:

1. Информационный портал по безопасности www.SecurityLab.ru.
2. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
3. Сайт Научной электронной библиотеки www.elibrary.ru
4. Справочно-правовая система «Гарант» » www.garant.ru
5. Справочно-правовая система «Консультант Плюс» www.consultant.ru

6. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
7. Федеральный портал «Российское образование www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Демонстрировать умениями практические навыки в подготовке оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями ,а также базами данных	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и

		результатов выполнения видов работ на практике
ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе	- многоуровневая защита сетей; - защита персональных компьютеров и компьютерных сетей; - практические методы и средства исследования сетей с целью поиска уязвимостей.	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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 Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
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	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно	- взаимодействие с обучающимися, преподавателями и	

взаимодействовать с коллегами, руководством, клиентами.	мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные	- эффективность использования	

технологии в профессиональной деятельности.	информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	