

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Романчук Иван Сергеевич

Должность: Ректор

Дата подписания: 19.09.2024 14:13:58

Уникальный программный ключ:

6319edc2b582ffdacea443f01d5779368d0957ac34f5cd074d81f81530452479

ФГАОУ ВО «Тюменский государственный университет»

Школа компьютерных наук

Кафедра Информационной безопасности

УТВЕРЖДЕНО

Заместителем директора школы,

А.В. Сапожниковой

РАЗРАБОТЧИК

А.А. Оленников

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

Рабочая программа профессионального модуля
включая междисциплинарные курсы (далее – МДК):

МДК.01.01 ОПЕРАЦИОННЫЕ СИСТЕМЫ

МДК.01.02 БАЗЫ ДАННЫХ

МДК.01.03 СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

МДК.01.04 ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ

АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специальность: 10.02.05 Обеспечение информационной безопасности

автоматизированных систем

Форма обучения: Очная

язык реализации: Русский

Тюмень, 2024

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
<p>ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4</p>	<p>31 состав и принципы работы автоматизированных систем, операционных систем и сред;</p> <p>32 принципы разработки алгоритмов программ, основных приемов программирования;</p> <p>33 модели баз данных;</p> <p>34 принципы построения, физические основы работы периферийных устройств;</p> <p>35 теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей,</p>	<p>У1 осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;</p> <p>У2 организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;</p> <p>У3 осуществлять конфигурирование, настройку компонент систем защиты информации</p>	<p>Н1 конфигурирования, настройки автоматизированных систем.</p> <p>Н2 производства монтажных работ;</p> <p>Н3 настройки компонент систем защиты информации;</p> <p>Н4 установки, адаптации и сопровождения типового программного обеспечения;</p> <p>Н5 обнаружение и устранение неисправностей.</p>

	<p> протоколов и принципов адресации; 36 порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; 37 принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации. </p>	<p> автоматизированных систем; У4 производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы У5 настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; У6 обеспечивать работоспособность, обнаруживать и устранять неисправности. </p>	
--	--	---	--

2. Структура и содержание профессионального модуля

Рабочая программа профессионального модуля ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» является обязательной частью образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по очной форме обучения.

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и учебным планом образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Цель профессионального модуля состоит в освоении знаний, приобретении умений, получении практического опыта и формировании компетенций в области защиты информации в автоматизированных системах программными и программно-аппаратными средствами.

2.1. Структура профессионального модуля

Наименования разделов профессионального модуля (МДК)	Семестр	Всего (ак.ч.)	В т.ч. в форме практической подготовки	Учебные занятия по МДК (всего ак.ч.)	Самостоятельная работа по МДК	Курсовые работы (проекты)	Форма промежуточной аттестации
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>
МДК.01.01 Операционные системы	2	108	–	72	30	–	Экзамен
МДК.01.02 Базы данных	2	108	–	72	30	–	Экзамен

МДК.01.03 Сети и системы передачи информации	3	136	–	88	42	–	Экзамен
МДК.01.04 Эксплуатация защищенных автоматизированных систем	3	72	–	60	4	–	Экзамен
Консультации				12			
Экзамен по модулю	3	6					Экзамен
Итого по ПМ:		430	–	292	106	–	Экзамен по модулю

2.2. Тематический план и содержание профессионального модуля

Содержание учебного материала	Вид учебной деятельности (ак.ч.)					
	Урок	Лекция	Практическое занятие (Семинар)	Лабораторное / Практическое занятие по	Выполнение курсового проекта (работы)	Самостоятельная работа
МДК.01.01 Операционные системы						
Семестр 2						
Раздел 1. Элементы теории операционных систем. Свойства операционных систем.						
Тема 1.1. Основы теории операционных систем		2		2		
Тема 1.2. Машиннозависимые и машиннонезависимые свойства операционных систем.		2		2		
Тема 1.3. Модульная структура операционных систем, пространство пользователя.		4		4		
Тема 1.4. Управление памятью.		2		2		
Тема 1.5. Управление процессами, многопроцессорные системы.		4		4		

Тема 1.6. Виртуализация и облачные технологии.		6		6		10
Раздел 2. Безопасность операционных систем.						
Тема 2.1. Принципы построения защиты информации в операционных системах.		4		4		6
Раздел 3. Особенности работы в современных операционных системах.						
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android.		4		4		4
Тема 3.2. Операционная система Windows.		4		4		4
Тема 3.3. Серверные операционные системы.		4		4		6
Консультации	2					
Промежуточная аттестация	экзамен (4 ак.ч)					
Всего		36		36		30
МДК.01.02 Базы данных						
Семестр 2						
Раздел 1. Основы теории баз данных.						
Тема 1.1. Основные понятия теории баз данных. Модели данных.		2		2		
Тема 1.2. Основы реляционной алгебры.		2		2		
Тема 1.3. Базовые понятия и классификация систем управления базами данных.		2		2		
Тема 1.4. Целостность данных как ключевое понятие баз данных.		2		2		
Раздел 2. Проектирование баз данных.						
Тема 2.1. Информационные модели реляционных баз данных.		2		2		
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.		2		2		
Тема 2.3. Средства автоматизации проектирования.		2		2		
Раздел 3. Организация баз данных.						
Тема 3.1. Создание базы данных. Манипулирование данными.		2		2		2
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц.		2		2		2
Раздел 4. Управление базой данных с помощью SQL.						
Тема 4.1. Структурированный язык запросов SQL.		2		2		2

Тема 4.2. Операторы и функции языка SQL.		2		2		2
Раздел 5. Организация распределённых баз данных.						
Тема 5.1. Архитектуры распределённых баз данных.		2		2		2
Тема 5.2. Серверная часть распределённой базы данных.		2		2		4
Тема 5.3. Клиентская часть распределённой базы данных.		2		2		4
Раздел 6. Администрирование и безопасность.						
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.		2		2		
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок.		2		2		4
Тема 6.3. Механизмы защиты информации в системах управления базами данных.		2		2		4
Тема 6.4. Копирование и перенос данных. Восстановление данных.		2		2		4
Консультации	2					
Промежуточная аттестация	экзамен (4 ак.ч)					
Всего		36		36		30
МДК.01.03 Сети и системы передачи информации						
Семестр 3						
Раздел 1. Теория телекоммуникационных сетей.						
Тема 1.1. Основные понятия и определения.		6				4
Тема 1.2. Принципы передачи информации в сетях и системах связи.		6		8		6
Тема 1.3. Типовые каналы передачи и их характеристики.		10		8		8
Раздел 2. Сети передачи данных.						
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных.		6		12		8
Тема 2.2. Беспроводные системы передачи данных.		6		10		8
Тема 2.3. Сотовые и спутниковые системы.		6		10		8
Консультации	2					
Промежуточная аттестация	экзамен (4 ак.ч)					
Всего		40		48		42
МДК.01.04 Эксплуатация защищённых автоматизированных систем						
Семестр 3						

Раздел 1. Разработка защищенных автоматизированных (информационных) систем.						
Тема 1.1. Основы информационных систем как объекта защиты.		2		2		
Тема 1.2. Жизненный цикл автоматизированных систем.		2		2		
Тема 1.3. Угрозы безопасности информации в автоматизированных системах.		2		2		
Тема 1.4. Основные меры защиты информации в автоматизированных системах.		2		2		
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении.		2		2		
Тема 1.6. Защита информации в распределенных автоматизированных системах.		2		2		
Тема 1.7. Особенности разработки информационных систем персональных данных.		2		2		
Раздел 2. Эксплуатация защищенных автоматизированных систем.						
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.		2		2		2
Тема 2.2. Администрирование автоматизированных систем.		2		4		
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении.		2		2		2
Тема 2.4. Защита от несанкционированного доступа к информации.		2		2		
Тема 2.5. СЗИ от НСД.		2		2		
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях.		2		4		
Тема 2.7. Документация на защищаемую автоматизированную систему.		2		2		
Консультации		4				
Промежуточная аттестация		экзамен (4 ак.ч)				
Всего		28		32		4
Всего по модулю		140		152		106

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК и в целом по модулю осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК.01.01 «Операционные системы» во 2 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных

ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.01.02 «Базы данных» во 2 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в

полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.01.03 «Сети и системы передачи информации» в 3 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для

получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.01.04 «Эксплуатация защищенных автоматизированных систем» в 3 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и

с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

4.1.1. Основная литература:

МДК.01.01 Операционные системы

1. 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, 2021. — 560 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-501-1. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1189335> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/557735> (дата обращения: 09.09.2024).

МДК.01.02 Базы данных

1. Мартишин, С. А. Базы данных: Работа с распределенными базами данных и файловыми системами на примере MongoDB и HDFS с использованием

Node.js, Express.js, Apache Spark и Scala : учебное пособие / С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. — Москва : ИНФРА-М, 2021. — 235 с. + Доп. материалы [Электронный ресурс]. — (Среднее профессиональное образование). - ISBN 978-5-16-015643-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189321> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1898839> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

МДК.01.03 Сети и системы передачи информации

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2130242> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мещатунян. — Москва : ФОРУМ : ИНФРА-М, 2024. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2138953> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

МДК.01.04 Эксплуатация защищенных автоматизированных систем

1. Цифровые технологии в учебном процессе : учебник (с электронными приложениями) / С. В. Алексахин, В. И. Блинов, И. С. Сергеев, В. А. Тармин. - Москва : РИОР : ИНФРА-М, 2023. - 311 с. - DOI: <https://doi.org/10.29039/01922-1>. - ISBN 978-5-369-01922-1. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2019008> (дата обращения: 09.09.2024)

2. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва ; Вологда : Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2169702> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

4.1.2. Дополнительная литература:

МДК.01.01 Операционные системы

1. Гвоздева, В. А. Информатика, автоматизированные информационные технологии и системы : учебник / В.А. Гвоздева. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2020. — 542 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0856-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1067007> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Голицына, О. Л. Информационные системы и технологии : учебное пособие / О.Л. Голицына, Н.В. Максимов, И.И. Попов. —Москва : ФОРУМ : ИНФРА-М, 2021. —400 с. —(Среднее профессиональное образование). -ISBN 978-5-00091-592-9. -Текст : электронный. -URL: <https://znanium.com/catalog/product/1138895> (дата обращения: 14.03.2022).

МДК.01.02 Базы данных

1. Немцова, Т. И. Практикум по информатике. Компьютерная графика и web-дизайн : учебное пособие / Т.И. Немцова, Ю.В. Назарова ; под ред. Л.Г. Гагариной. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2020. — 288 с. + Доп. материалы [Электронный ресурс]. — (Среднее профессиональное образование). - ISBN 978-5-8199-0800-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1073058> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Гмурман, В. Е. Руководство к решению задач по теории вероятностей и математической статистике : учебное пособие для среднего профессионального образования / В. Е. Гмурман. — 11-е изд., перераб. и доп. — Москва : Издательство

Юрайт, 2020. — 406 с. — (Профессиональное образование). — ISBN 978-5-534-08569-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/451168> (дата обращения: 10.09.2024).

МДК.01.03 Сети и системы передачи информации

1. 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 ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512861> (дата обращения: 09.09.2024).

2. Алиев, И. И. Электротехника и электрооборудование: базовые основы : учебное пособие для среднего профессионального образования / И. И. Алиев. — 5-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 291 с. — (Профессиональное образование). — ISBN 978-5-534-04256-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539388> (дата обращения: 09.09.2024).

3. Миленина, С. А. Электротехника, электроника и схемотехника : учебник и практикум для среднего профессионального образования / С. А. Миленина, Н. К. Миленин ; под редакцией Н. К. Миленина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 406 с. — (Профессиональное образование). — ISBN 978-5-534-04676-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536766> (дата обращения: 09.09.2024).

МДК.01.04 Эксплуатация защищенных автоматизированных систем

1. Гагарина, Л. Г. Технические средства информатизации : учебное пособие / Л.Г. Гагарина, Ф.С. Золотухин. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2021. — 260 с. — (Среднее профессиональное образование). — DOI 10.12737/1083293. -ISBN 978-5-16-016140-2. -Текст : электронный. -URL:

<https://znanium.com/catalog/product/1083293> (дата обращения: 21.04.2023). –Режим доступа: по подписке.

2. Максимов, Н. В. Технические средства информатизации : учебник / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. —4-е изд., перераб. и доп. —М. : ФОРУМ : ИНФРА-М, 2019. —608 с. —(Профессиональное образование). -ISBN 978-5-91134-763-5. -Текст : электронный // ЭБС ZNANIUM.COM: сайт. -URL: <https://znanium.com/catalog/product/1033885> (дата обращения: 06.04.2023).

4.1.3. Современные профессиональные базы данных и информационные справочные системы:

- Научная электронная библиотека eLIBRARY.RU;
- Springer;
- JSTOR;
- База данных ООО «ИВИС»;
- База данных IPR Books;
- Образовательная платформа Юрайт.

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

LibreOffice, платформы: Яндекс. Мессенджер, Яндекс.Телемост.

4.3. Материально-техническое обеспечение реализации дисциплины:

Кабинет информационных технологий, программирования и баз данных.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран.

Программное обеспечение: платформа Яндекс 360 (телемост, мессенджер), операционная система Альт Образование, офисный пакет Libre Office (Writer, Impress, Draw, Base, Calc, Math), сетевые браузеры Chromium, Яндекс Браузер. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС,

электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения групповых и индивидуальных консультаций.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная.

Технические средства обучения: персональный компьютер, проектор, звуковой усилитель, колонки, экран.

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения промежуточной и итоговой аттестации.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для организации самостоятельной и воспитательной работы.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ
МОДУЛЮ
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ
(ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ
МДК.01.01 ОПЕРАЦИОННЫЕ СИСТЕМЫ
МДК.01.02 БАЗЫ ДАННЫХ
МДК.01.03 СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ
МДК.01.04 ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Открытая часть**

1. Система оценивания

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК.01.01 «Операционные системы» во 2 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ

должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.01.02 «Базы данных» во 2 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.01.03 «Сети и системы передачи информации» в 3 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения

студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.01.04 «Эксплуатация защищенных автоматизированных систем» в 3 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы (виды и количество)	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.01.01 Операционные системы			
Текущий контроль успеваемости			
Тема 1.1. Основы теории операционных систем	Лабораторная работа	ОК 01. Выбирать способы решения задач	5 баллов
Тема 1.2. Машиннозависимые и машиннонезависимые свойства операционных систем.	Лабораторная работа	профессиональной деятельности применительно к различным контекстам;	5 баллов
Тема 1.3. Модульная структура операционных систем,	Лабораторная работа	ОК 02. Использовать современные средства поиска, анализа и	10 баллов

пространство пользователя.		интерпретации информации и	
Тема 1.4. Управление памятью.	Лабораторная работа	информационные технологии для	10 баллов
Тема 1.5. Управление процессами, многопроцессорные системы.	Лабораторная работа	выполнения задач профессиональной деятельности;	10 баллов
Тема 1.6. Виртуализация и облачные технологии.	Лабораторная работа	ОК 03. Планировать и реализовывать собственное профессиональное и	10 баллов
Тема 2.1. Принципы построения защиты информации в операционных системах.	Лабораторная работа	личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать	15 баллов
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android.	Лабораторная работа	знания по правовой и финансовой грамотности в	15 баллов
Тема 3.2. Операционная система Windows.	Лабораторная работа	различных жизненных ситуациях;	15 баллов
		ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;	15 баллов
		ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;	
		ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных	

		<p>ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;</p> <p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;</p> <p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;</p> <p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.</p> <p>ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном</p>	
--	--	---	--

		исполнении соответствии требованиями эксплуатационной документации.	в с
Промежуточная аттестация обучающихся			
Экзамен	2 семестр	ОК 01 – ОК 09, ПК 1.1	
МДК.01.02 Базы данных			
Текущий контроль успеваемости			
Тема 1.1. Основные понятия теории баз данных. Модели данных.	Лабораторная работа	ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;	5 баллов
Тема 1.2. Основы реляционной алгебры.	Лабораторная работа	ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;	5 баллов
Тема 1.3. Базовые понятия и классификация систем управления базами данных.	Лабораторная работа	ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;	5 баллов
Тема 1.4. Целостность данных как ключевое понятие баз	Лабораторная работа	ОК 04. Эффективно взаимодействовать и	5 баллов
Тема 2.1. Информационные модели реляционных баз данных.	Лабораторная работа		5 баллов
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	Лабораторная работа		5 баллов
Тема 2.3. Средства автоматизации проектирования.	Лабораторная работа		5 баллов
Тема 3.1. Создание базы данных. Манипулирование данными.	Лабораторная работа		5 баллов
Тема 3.2. Индексы. Связи между таблицами.	Лабораторная работа		5 баллов

Тема 4.1. Структурированный язык запросов SQL.	Лабораторная работа	работать в коллективе и команде; ОК 05. Осуществлять	5 баллов
Тема 4.2. Операторы и функции языка SQL.	Лабораторная работа	устную и письменную коммуникацию на	5 баллов
Тема 5.1. Архитектуры распределенных баз данных.	Лабораторная работа	государственном языке Российской Федерации с учетом	5 баллов
Тема 5.2. Серверная часть распределенной базы данных.	Лабораторная работа	особенностей социального и культурного	5 баллов
Тема 5.3. Клиентская часть распределенной базы данных.	Лабораторная работа	контекста; ОК 06. Проявлять	5 баллов
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	Лабораторная работа	гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе	5 баллов
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок.	Лабораторная работа	традиционных российских духовно-нравственных ценностей, в том числе	5 баллов
Тема 6.3. Механизмы защиты информации в системах управления базами данных.	Лабораторная работа	с учетом гармонизации межнациональных и межрелигиозных	5 баллов
Тема 6.4. Копирование и перенос данных. Восстановление данных.	Лабораторная работа	отношений, применять стандарты антикоррупционного поведения; ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;	5 баллов

		<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;</p> <p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.</p> <p>ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.</p>	
Промежуточная аттестация обучающихся			
Экзамен	2 семестр	ОК 01 – ОК 09, ПК 1.1	
МДК.01.03 Сети и системы передачи информации			
Тема 1.2. Принципы передачи информации в сетях и системах связи.	Лабораторная работа	ОК 01. Выбирать способы решения задач профессиональной деятельности	10 баллов
Тема 1.3. Типовые каналы передачи и их характеристики.	Лабораторная работа	применительно к различным	10 баллов
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных.	Лабораторная работа	контекстам; ОК 02. Использовать современные средства поиска, анализа и	10 баллов

Тема 2.2. Беспроводные системы передачи данных.	Лабораторная работа	интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;	20 баллов
Тема 2.3. Сотовые и спутниковые системы.	Лабораторная работа	ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях; ОК 04. Эффективно взаимодействовать и работать в коллективе и команде; ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста; ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных	20 баллов

		<p>ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;</p> <p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;</p> <p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;</p> <p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.</p> <p>ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном</p>	
--	--	---	--

		исполнении соответствии требованиями эксплуатационной документации. ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении соответствии требованиями эксплуатационной документации. ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	В С В С и
Промежуточная аттестация обучающихся			
Экзамен	3 семестр	ОК 01 – ОК 09, ПК 1.1, ПК 1.3, ПК 1.4	
МДК.01.04 Эксплуатация защищенных автоматизированных систем			
Тема 1.1. Основы информационных систем как объекта защиты.	Лабораторная работа	ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;	5 баллов
Тема 1.2. Жизненный цикл автоматизированных систем.	Лабораторная работа	ОК 02. Использовать современные средства поиска, анализа и	5 баллов
Тема 1.3. Угрозы безопасности информации	Лабораторная работа		5 баллов

автоматизированных системах.		интерпретации информации и	
Тема 1.4. Основные меры защиты информации в автоматизированных системах.	Лабораторная работа	информационные технологии для выполнения задач профессиональной деятельности;	5 баллов
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении.	Лабораторная работа	ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие,	5 баллов
Тема 1.6. Защита информации в распределенных автоматизированных системах.	Лабораторная работа	предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и	5 баллов
Тема 1.7. Особенности разработки информационных систем персональных данных.	Лабораторная работа	финансовой грамотности в различных жизненных ситуациях;	5 баллов
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Лабораторная работа	ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;	5 баллов
Тема 2.2. Администрирование автоматизированных систем.	Лабораторная работа	ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом	5 баллов
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении.	Лабораторная работа	особенностей социального и культурного контекста;	5 баллов
Тема 2.4. Защита от несанкционированного доступа к информации.	Лабораторная работа	ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение	5 баллов
Тема 2.5. СЗИ от НСД.	Лабораторная работа	на основе традиционных	5 баллов

<p>Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях.</p>	<p>Лабораторная работа</p>	<p>российских духовно-нравственных ценностей, в том числе с учетом</p>	<p>5 баллов</p>
<p>Тема 2.7. Документация на защищаемую автоматизированную систему.</p>	<p>Лабораторная работа</p>	<p>гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения; ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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. Пользоваться профессиональной документацией на государственном и иностранном языках. ПК 1.1. Производить установку и настройку компонентов автоматизированных</p>	<p>5 баллов</p>

		<p>(информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.</p> <p>ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.</p> <p>ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.</p> <p>ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.</p>	
Промежуточная аттестация обучающихся			

Экзамен	3 семестр	ОК 01 – ОК 09, ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4	
Экзамен по модулю	3 семестр	ОК 01 – ОК 09, ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4	

3. Типовые оценочные материалы

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК 01.01 Операционные системы.

1. Определение операционной системы.
2. История развития операционных систем.
3. Виды операционных систем.
4. Классификация операционных систем по разным признакам.
5. Операционная система как интерфейс между программным и аппаратным обеспечением.
6. Системные вызовы.
7. Исследования в области операционных систем.
8. Загрузчик ОС.
9. Инициализация аппаратных средств.
10. Процесс загрузки ОС.
11. Переносимость ОС.
12. Машинно-зависимые модули ОС.
13. Задачи ОС по управлению операциями ввода-вывода.
14. Многослойная модель подсистемы ввода-вывода.
15. Драйверы.
16. Поддержка операций ввода-вывода.
17. Работа с файлами.
18. Файловая система.
19. Виды файловых систем.
20. Физическая организация файловой системы.
21. Типы файлов.
22. Файловые операции
23. Контроль доступа к файлам.
24. Модель клиент-сервер.
25. Работа в режиме пользователя.
26. Работа в консольном режиме.
27. Оболочки операционных систем.
28. Основное управление памятью.
29. Виртуальная память.
30. Алгоритмы замещения страниц.
31. Сегментация памяти.
32. Понятие процесса.
33. Понятие потока.

34. Понятие приоритета и очереди процессов,
35. Особенности многопроцессорных систем.
36. Межпроцессорное взаимодействие
37. Понятие взаимоблокировки.
38. Ресурсы, обнаружение взаимоблокировок.
39. Избегание взаимоблокировок.
40. Предотвращение взаимоблокировок
41. Требования, применяемые к виртуализации.
42. Гипервизоры.
43. Технологии эффективной виртуализации.
44. Виртуализация памяти.
45. Виртуализация ввода-вывода.
46. Виртуальные устройства.
47. Вопросы лицензирования
48. Облачные технологии.
49. Исследования в области виртуализации и облаков
50. Понятие безопасности ОС.
51. Классификация угроз ОС.
52. Источники угроз информационной безопасности и объекты воздействия.
53. Порядок обеспечения безопасности информации при эксплуатации операционных систем.
54. Штатные средства ОС для защиты информации.
55. Аутентификация,
56. Авторизация
57. Аудит.
58. Обзор системы Linux.
59. Процессы в системе Linux.
60. Управление памятью в Linux.
61. Ввод-вывод в системе Linux.
62. Файловая система UNIX.
63. Архитектура Android.
64. Структура системы.
65. Процессы и потоки в Windows.
66. Управление памятью.
67. Ввод-вывод в Windows.
68. Основное назначение серверных ОС.
69. Особенности серверных ОС.
70. Распределенные файловые системы

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК 01.02 Базы данных.

1. Понятие базы данных.
2. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи.

3. Однопользовательские и многопользовательские системы баз данных.
4. Интегрированные и общие данные.
5. Объекты, свойства, отношения.
6. Централизованное управление данными, основные требования.
7. Модели данных.
8. Иерархические, сетевые и реляционные модели организации данных.
9. Постреляционные модели данных.
10. Терминология реляционных моделей.
11. Классификация сущностей.
12. Двенадцать правил Кодда для определения концепции реляционной модели.
13. Основы реляционной алгебры.
14. Традиционные операции над отношениями.
15. Специальные операции над отношениями.
16. Операции над отношениями дополненные Дейтом.
17. Основные функции, реализуемые в СУБД.
18. Основные компоненты СУБД и их взаимодействие.
19. Интерфейс СУБД.
20. Языковые средства СУБД.
21. Классификация СУБД.
22. Понятие целостности и непротиворечивости данных.
23. Примеры нарушения целостности и непротиворечивости данных.
24. Правила и ограничения.
25. Типы информационных моделей.
26. Логические модели данных.
27. Физические модели данных.
28. Необходимость нормализации.
29. Аномалии вставки, удаления и обновления.
30. Применение процесса нормализации.
31. CASE-средства,
32. CASE-система
33. CASE-технология.
34. Классификация CASE-средств.
35. Графическое представление моделей проектирования. UML.
36. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.
37. Создание базы данных.
38. Работа с таблицами: создание таблицы
39. Работа с таблицами: изменение структуры
40. Работа с таблицами: наполнение таблицы данными.
41. Управление записями: добавление
42. Управление записями: редактирование
43. Управление записями: удаление и навигация.
44. Работа с базой данных: восстановление и сжатие.
45. Открытие и модификация данных.

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК.01.03 Сети и системы передачи информации.

1. Классификация систем связи.
2. Сообщения и сигналы.
3. Виды электронных сигналов.
4. Спектральное представление сигналов.
5. Параметры сигналов.
6. Объем и информационная емкость сигнала.
7. Назначение и принципы организации сетей.
8. Классификация сетей.
9. Многоуровневый подход.
10. Протокол. Интерфейс.
11. Стек протоколов.
12. Телекоммуникационная среда.
13. Канал передачи.
14. Сетевой тракт, групповой канал передачи.
15. Аппаратура цифровых плезиохронных систем передачи.
16. Основные параметры и характеристики сигналов.
17. Упрощенная схема организации канала ТЧ
18. Структура и характеристики сетей.
19. Способы коммутации и передачи данных.
20. Распределение функций по системам сети и адресация пакетов.
21. Маршрутизация и управление потоками в сетях связи.
22. Протоколы и интерфейсы управления каналами и сетью передачи данных.
23. Беспроводные каналы связи.
24. Беспроводные сети Wi-Fi.
25. Преимущества и область применения.
26. Основные элементы беспроводных сетей.
27. Стандарты беспроводных сетей.
28. Технология WIMAX
29. Принципы функционирования систем сотовой связи.
30. Стандарты GSM и CDMA.

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК.01.04 Эксплуатация защищенных автоматизированных систем.

1. Понятие автоматизированной (информационной) системы
2. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу,
3. Отличительные черты АИС наиболее часто используемых классификаций: в зависимости от характера информационных ресурсов.
4. Отличительные черты АИС наиболее часто используемых классификаций: по технологии обработки данных.

5. Отличительные черты АИС наиболее часто используемых классификаций: по способу доступа.
6. Отличительные черты АИС наиболее часто используемых классификаций: в зависимости от организации системы.
7. Отличительные черты АИС наиболее часто используемых классификаций: по характеру использования информации.
8. Отличительные черты АИС наиболее часто используемых классификаций: по сфере применения.
9. Примеры областей применения АИС.
10. Процессы в АИС: ввод,
11. Процессы в АИС: обработка,
12. Процессы в АИС: вывод,
13. Процессы в АИС: обратная связь.
14. Требования к АИС: гибкость,
15. Требования к АИС: надежность,
16. Требования к АИС: эффективность,
17. Требования к АИС: безопасность.
18. Основные особенности современных проектов АИС.
19. Электронный документооборот.
20. Понятие жизненного цикла АИС.
21. Процессы жизненного цикла АИС: основные
22. Процессы жизненного цикла АИС: вспомогательные
23. Процессы жизненного цикла АИС: организационные.
24. Стадии жизненного цикла АИС: моделирование,
25. Стадии жизненного цикла АИС: управление требованиями
26. Стадии жизненного цикла АИС: анализ и проектирование
27. Стадии жизненного цикла АИС: установка и сопровождение.
28. Модели жизненного цикла АИС.
29. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении.
30. Методологии проектирования.
31. Организация работ
32. Функции заказчиков и разработчиков.
33. Требования к автоматизированной системе в защищенном исполнении.
34. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении.
35. Требования по защите сведений о создаваемой автоматизированной системе.
36. Потенциальные угрозы безопасности в автоматизированных системах.
37. Источники и объекты воздействия угроз безопасности информации.
38. Критерии классификации угроз.
39. Методы оценки опасности угроз.
40. Банк данных угроз безопасности информации
41. Понятие уязвимости угрозы.
42. Классификация уязвимостей.

43. Организационные меры защиты информации в автоматизированных системах
44. Правовые меры защиты информации в автоматизированных системах
45. Программно-аппаратные меры защиты информации в автоматизированных системах
46. Криптографические меры защиты информации в автоматизированных системах
47. Технические меры защиты информации в автоматизированных системах.
48. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним
49. Идентификация и аутентификация субъектов доступа и объектов доступа.
50. Управление доступом субъектов доступа к объектам доступа.
51. Ограничение программной среды.
52. Антивирусная защита.
53. Резервное копирование
54. Восстановление данных.
55. Механизмы и методы защиты информации в распределенных автоматизированных системах.
56. Архитектура механизмов защиты распределенных автоматизированных систем.
57. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.
58. Общие требования по защите персональных данных.
59. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.
60. Порядок выбора мер по обеспечению безопасности персональных данных.
61. Требования по защите персональных данных, в соответствии с уровнем защищенности.
62. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.
63. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.
64. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении.
65. Задачи и функции администрирования автоматизированных систем.
66. Автоматизация управления сетью.
67. Организация администрирования автоматизированных систем.
68. Административный персонал и работа с пользователями.
69. Управление, тестирование и эксплуатация автоматизированных систем.
70. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
71. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.

72. Общие обязанности администратора информационной безопасности автоматизированных систем.
73. Основные принципы защиты от НСД.
74. Основные способы НСД.
75. Основные направления обеспечения защиты от НСД.
76. Основные характеристики технических средств защиты от НСД.
77. Организация работ по защите от НСД.
78. Классификация автоматизированных систем.
79. Требования по защите информации от НСД для АС
80. Требования защищенности СВТ от НСД к информации.

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по ПМ 01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении»

Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти.

1. Резервное копирование и восстановление данных.
2. Принципы функционирования систем сотовой связи.
3. Сеть 192.168.1.0 / 24 необходимо разделить на 2 части, а потом одну из сетей поделить еще на 4 подсети.
4. Стандарты GSM и CDMA. Спутниковые системы передачи данных.
5. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.
6. Использование построителя выражений.
7. К какому классу IP-адресов относится IP-адрес: 198.64.56.98. Напишите маску подсети.
8. Технология разработки форм. Назначение, виды, способы создания, структура.
9. Структура и характеристики сетей. Способы коммутации и передачи данных.
10. Защита технических средств.
11. К какому классу IP-адресов относится IP-адрес: 198.64.56.98. Напишите маску подсети.
12. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.
13. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ
14. Термины и определения реляционных баз данных.
15. Сеть 192.168.1.0 / 24 необходимо разделить на 2 части, а потом одну из сетей поделить еще на 4 подсети.
16. Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux.
17. Ввод-вывод в системе Linux. Файловая система UNIX.

18. Основные понятия распределенной обработки данных. Режимы работы с базами данных
19. Перекрестный запрос. Назначение, создание, примеры.
20. Сеть 10.10.0.0 / 15 разбить на 8 частей.
21. Виды электронных сигналов.
22. Редактирование запроса.
23. Условия работы удаленного доступа к данным.
24. Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.
25. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные.
26. Классификация систем связи. Сообщения и сигналы
27. Сформировать список программных и аппаратных серверов, которые могла бы использовать малая или средняя фирма для решения своих задач в области внутренней коммуникации и обмена информацией внутри локальной сети.
28. Основные элементы беспроводных сетей. Стандарты беспроводных сетей.
29. Идентификация и аутентификация субъектов доступа и объектов доступа.
30. Итоговые запросы. Назначение, создание, примеры
31. Сеть 10.10.0.0 / 15 разбить на 8 частей.
32. Обеспечение целостности информационной системы и информации
33. Технология WIMAX
34. Операционные системы семейства Mac OS: особенности, преимущества и недостатки.
35. 45. На сколько подсетей можно разделить Ip 12.34.56.78 с маской 255.255.224.0?
36. Дополнительные функции защиты от петель. Агрегирование каналов связи.
37. Понятие автоматизированной (информационной) системы
38. К какому классу IP-адресов относится IP-адрес: 198.64.56.98. Напишите маску подсети.
39. Модель удаленного управления данными. Двухуровневая модель, расположение, распределение функций, алгоритм выполнения клиентского запроса.
40. Технология PoweroverEthernet
41. Упрощенная схема организации канала ГЧ
42. Сеть 192.168.1.0 / 24 необходимо разделить на 2 части, а потом одну из сетей поделить еще на 4 подсети.
43. Сверхвысокоскоростные сети
44. Ввод и анализ данных с помощью форм. Назначение, способ организации.
45. Процессор управления данными. Расположение, модели распределений.
46. Телекоммуникационная среда.

ФГАОУ ВО «Тюменский государственный университет»
Школа компьютерных наук
Кафедра Информационной безопасности

УТВЕРЖДЕНО
Заместителем директора школы,
А.В. Сапожниковой
РАЗРАБОТЧИК
А.А. Оленников

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

Рабочая программа профессионального модуля
включая междисциплинарные курсы (далее – МДК):

**МДК.02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ
СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ**

**МДК.02.02 КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ
ИНФОРМАЦИИ**

Специальность: 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Форма обучения: Очная
язык реализации: Русский

Тюмень, 2024

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
<p>ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4, ПК2.5, ПК2.6.</p>	<p>31 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</p> <p>32 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;</p> <p>33 типовые модели управления доступом, средств, методов и протоколов</p>	<p>У1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</p> <p>У2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;</p> <p>У3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</p> <p>У4 применять программные и программно-аппаратные средства для</p>	<p>Н1 установки и настройки, программные и программно-аппаратных средств защиты информации;</p> <p>Н2 настройки средств антивирусной защиты;</p> <p>Н3 устранения отказов оборудования;</p> <p>Н4 применения программных и программно-аппаратных средств;</p> <p>Н5 применения математических аппаратов для выполнения криптографических преобразований.</p>

	<p>идентификации и аутентификации;</p> <p>34 основные понятия криптографии и типовых криптографических методов и средств защиты информации;</p> <p>35 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;</p> <p>36 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.</p>	<p>защиты информации в базах данных;</p> <p>У5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;</p> <p>У6 применять математический аппарат для выполнения криптографических преобразований;</p> <p>У7 использовать типовые программные криптографические средства, в том числе электронную подпись;</p> <p>У8 применять средства гарантированного</p>	
--	--	--	--

		<p>уничтожения информации;</p> <p>У9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</p> <p>У10 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.</p>	
--	--	--	--

2. Структура и содержание профессионального модуля

Рабочая программа профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными

средствами» является обязательной частью образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по очной форме обучения.

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и учебным планом образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Цель профессионального модуля состоит в освоении знаний, приобретении умений, получении практического опыта и формировании компетенций в области защиты информации в автоматизированных системах программными и программно-аппаратными средствами.

2.1. Структура профессионального модуля

Наименования разделов профессионального модуля (МДК)	Семестр	Всего (ак.ч.)	В т.ч. в форме практической подготовки	Учебные занятия по МДК (всего ак.ч.)	Самостоятельная работа по МДК	Курсовые работы (проекты)	Форма промежуточной аттестации
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>
МДК.02.01 Программные и программно-аппаратные средства защиты информации	4	188	–	98	88	–	Зачет, курсовая работа
МДК.02.02 Криптографические средства защиты информации	4	160	–	102	52	–	Экзамен
Консультации					6		
Экзамен по модулю	4	6					Экзамен

Итого по ПМ:		354	–	200	140	–	Экзамен по модулю
---------------------	--	------------	----------	------------	------------	----------	--------------------------

2.2. Тематический план и содержание профессионального модуля

Содержание учебного материала	Вид учебной деятельности (ак.ч.)					
	Урок	Лекция	Практическое занятие (Семинар)	Лабораторное / Практическое занятие по	Выполнение курсового проекта (лаборт)	Самостоятельная работа
МДК.02.01 Программные и программно-аппаратные средства защиты информации.						
Семестр 4						
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации.						
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации.		2	2			
Тема 1.2. Стандарты безопасности.		2	2			
Тема 1.3. Защищенная автоматизированная система.		2	2			
Тема 1.4. Дестабилизирующее воздействие на объекты защиты.		2	2			
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа.		2	2			
Раздел 2. Защита автономных автоматизированных систем.						
Тема 2.1. Основы защиты автономных автоматизированных систем.		2	2			
Тема 2.2. Защита программ от изучения.		2	2			
Тема 2.3. Вредоносное программное обеспечение.		2	2			

Тема 2.4. Защита программ и данных от несанкционированного копирования.		2	2			
Тема 2.5. Защита информации на машинных носителях.		2	2			
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей.		2	2			
Тема 2.7. Системы обнаружения атак и вторжений.		2	2			8
Раздел 3. Защита информации в локальных сетях.						
Тема 3.1. Основы построения защищенных сетей.		2	2		4	10
Тема 3.2. Средства организации VPN.		2	4		2	6
Раздел 4. Защита информации в сетях общего доступа.						
Тема 4.1. Обеспечение безопасности межсетевое взаимодействия.		4	4		4	10
Раздел 5. Защита информации в базах данных.						
Тема 5.1. Защита информации в базах данных.		4	4		4	10
Раздел 6. Мониторинг систем защиты.						
Тема 6.1. Мониторинг систем защиты.		4	4		4	10
Тема 6.2. Изучение мер защиты информации в информационных системах.		4	4			10
Тема 6.3. Изучение современных программно-аппаратных комплексов.		4	4			6
Консультации		2				
Промежуточная аттестация		зачет, курсовая работа				
Всего		48	50		18	70
МДК.02.02 Криптографические средства защиты информации.						
Семестр 4						
Раздел 1. Математические основы защиты информации.						
Тема 1.1. Математические основы криптографии.		4	4			
Раздел 2. Классическая криптография.						
Тема 2.1. Методы криптографического защиты информации.		4	4			4
Тема 2.2. Криптоанализ.		4	4			4
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел.		4	4			
Раздел 3. Современная криптография.						
Тема 3.1. Кодирование информации. Компьютеризация шифрования.		4	4			

Тема 3.2. Симметричные системы шифрования.		4	4			8
Тема 3.3. Асимметричные системы шифрования.		4	4			8
Тема 3.4. Аутентификация данных. Электронная подпись.		4	4			8
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации.		4	4			8
Тема 3.6. Криптозащита информации в сетях передачи данных.		4	4			6
Тема 3.7. Защита информации в электронных платежных системах.		4	6			6
Тема 3.8. Компьютерная стеганография.		6	6			
Консультации	2					
Промежуточная аттестация	экзамен					
Всего		50	52			52
Всего по модулю		98	102			122

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК и в целом по модулю осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК.02.01 «Программные и программно-аппаратные средства защиты информации» в 4 семестре предусмотрен зачет. Зачет является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

- от 0 до 60 баллов – «не зачтено»;
- от 61 до 100 баллов – «зачтено».

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.02.02 «Криптографические средства защиты информации» в 4 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практических работ и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

4.1.1. Основная литература:

МДК.02.01 Программные и программно-аппаратные средства защиты информации

1. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва ; Вологда : Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2169702> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543631> (дата обращения: 09.09.2024).

МДК.02.02 Криптографические средства защиты информации

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1898839> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Цифровые технологии в учебном процессе : учебник (с электронными приложениями) / С. В. Алексахин, В. И. Блинов, И. С. Сергеев, В. А. Тармин. - Москва : РИОР : ИНФРА-М, 2023. - 311 с. - DOI: <https://doi.org/10.29039/01922-1>. - ISBN 978-5-369-01922-1. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2019008> (дата обращения: 09.09.2024).

4.1.2. Дополнительная литература:

МДК.02.01 Программные и программно-аппаратные средства защиты информации

1. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные

редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/555949> (дата обращения: 09.09.2024).

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2130242> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

МДК.02.02 Криптографические средства защиты информации

1. Гмурман, В. Е. Руководство к решению задач по теории вероятностей и математической статистике : учебное пособие для среднего профессионального образования / В. Е. Гмурман. — 11-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 406 с. — (Профессиональное образование). — ISBN 978-5-534-08569-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/451168> (дата обращения: 10.09.2024).

2. Омельченко, В. П. Математика : учебник / В.П. Омельченко, Н.В. Карасенко. — Москва : ИНФРА-М, 2024. — 349 с. — (Среднее профессиональное образование). — DOI 10.12737/1855784. - ISBN 978-5-16-017462-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2085068> (дата обращения: 10.09.2024). – Режим доступа: по подписке.

4.1.3. Современные профессиональные базы данных и информационные справочные системы:

- Научная электронная библиотека eLIBRARY.RU;
- Springer;
- JSTOR;
- База данных ООО «ИВИС»;
- База данных IPR Books;
- Образовательная платформа Юрайт.

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

LibreOffice, платформы: Яндекс. Мессенджер, Яндекс.Телемост.

4.3. Материально-техническое обеспечение реализации дисциплины:

Кабинет информационных технологий, программирования и баз данных.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран.

Программное обеспечение: платформа Яндекс 360 (телемост, мессенджер), операционная система Альт Образование, офисный пакет Libre Office (Writer, Impress, Draw, Base, Calc, Math), сетевые браузеры Chromium, Яндекс Браузер. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения групповых и индивидуальных консультаций.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная.

Технические средства обучения: персональный компьютер, проектор, звуковой усилитель, колонки, экран.

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения промежуточной и итоговой аттестации.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для организации самостоятельной и воспитательной работы.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ
МОДУЛЮ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ
СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-
АППАРАТНЫМИ СРЕДСТВАМИ**

**МДК.02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ
СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
МДК.02.02 КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ
ИНФОРМАЦИИ
Открытая часть**

1. Система оценивания

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК.02.01 «Программные и программно-аппаратные средства защиты информации» в 4 семестре предусмотрен зачет. Зачет является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

- от 0 до 60 баллов – «не зачтено»;
- от 61 до 100 баллов – «зачтено».

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен

выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.02.02 «Криптографические средства защиты информации» в 4 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы (виды и количество)	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.02.01 Программные и программно-аппаратные средства защиты информации			
Текущий контроль успеваемости			
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации.	Практическая работа	ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам; ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности; ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях; ОК 04. Эффективно взаимодействовать и	5 баллов
Тема 1.2. Стандарты безопасности.	Практическая работа		5 баллов
Тема 1.3. Защищенная автоматизированная система.	Практическая работа		5 баллов
Тема 1.4. Дестабилизирующее воздействие на объекты защиты.	Практическая работа		5 баллов
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа.	Практическая работа		5 баллов
Тема 2.1. Основы защиты автономных автоматизированных систем.	Практическая работа		5 баллов
Тема 2.2. Защита программ от изучения.	Практическая работа		5 баллов
Тема 2.3. Вредоносное программное обеспечение.	Практическая работа		5 баллов
Тема 2.4. Защита программ и данных от несанкционированного копирования.	Практическая работа		5 баллов
Тема 2.5. Защита информации на машинных носителях.	Практическая работа		5 баллов

Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей.	Практическая работа	работать в коллективе и команде; ОК 05. Осуществлять устную и письменную коммуникацию на	5 баллов
Тема 2.7. Системы обнаружения атак и вторжений.	Практическая работа	государственном языке Российской Федерации с учетом	5 баллов
Тема 3.1. Основы построения защищенных сетей.	Практическая работа	особенностей социального и культурного	5 баллов
Тема 3.2. Средства организации VPN.	Практическая работа	контекста; ОК 06. Проявлять	5 баллов
Тема 4.1. Обеспечение безопасности межсетевых взаимодействия.	Практическая работа	гражданско-патриотическую позицию, демонстрировать	5 баллов
Тема 5.1. Защита информации в базах данных.	Практическая работа	осознанное поведение на основе традиционных	5 баллов
Тема 6.1. Мониторинг систем защиты.	Практическая работа	российских духовно-нравственных	5 баллов
Тема 6.2. Изучение мер защиты информации в информационных системах.	Практическая работа	ценностей, в том числе с учетом гармонизации	5 баллов
Тема 6.3. Изучение современных программно-аппаратных комплексов.	Практическая работа	межрелигиозных отношений, применять стандарты антикоррупционного поведения; ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;	5 баллов

		<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;</p> <p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.</p> <p>ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.</p> <p>ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.</p> <p>ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.</p> <p>ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.</p>	
--	--	--	--

		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.	
Промежуточная аттестация обучающихся			
Зачет	4 семестр	ОК 01 – ОК 09, ПК 2.1 – ПК 2.6	
МДК.02.02 Криптографические средства защиты информации			
Текущий контроль успеваемости			
Тема 1.1. Математические основы криптографии.	Практическая работа	ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;	5 баллов
Тема 2.1. Методы криптографического защиты информации.	Практическая работа	ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач	5 баллов
Тема 2.2. Криптоанализ.	Практическая работа		5 баллов
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел.	Практическая работа		5 баллов
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Практическая работа		5 баллов

Тема 3.2. Симметричные системы шифрования.	Практическая работа	профессиональной деятельности; ОК 03. Планировать и	5 баллов
Тема 3.3. Асимметричные системы шифрования.	Практическая работа	реализовывать собственное профессиональное и	5 баллов
Тема 3.4. Аутентификация данных. Электронная подпись.	Практическая работа	личностное развитие, предпринимательскую деятельность в профессиональной	5 баллов
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации.	Практическая работа	сфере, использовать знания по правовой и финансовой грамотности в	5 баллов
Тема 3.6. Криптозащита информации в сетях передачи данных.	Практическая работа	различных жизненных ситуациях; ОК 04. Эффективно взаимодействовать и	5 баллов
Тема 3.7. Защита информации в электронных платежных системах.	Практическая работа	работать в коллективе и команде; ОК 05. Осуществлять устную и письменную	5 баллов
Тема 3.8. Компьютерная стеганография.	Практическая работа	коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста; ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных	5 баллов

		<p>отношений, применять стандарты антикоррупционного поведения; ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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. Пользоваться профессиональной документацией на государственном и иностранном языках. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.</p>	
Промежуточная аттестация обучающихся			
Экзамен	4 семестр	ОК 01 – ОК 09, ПК 2.4	
Экзамен по модулю	4 семестр	ОК 01 – ОК 09, ПК 2.1 – ПК 2.6	

3. Типовые оценочные материалы

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК.02.01 Программные и программно-аппаратные средства защиты информации.

1. Вредоносное программное обеспечение как особый вид разрушающих воздействий
2. Классификация вредоносного программного обеспечения.
3. Схема заражения.
4. Средства нейтрализации вредоносного ПО.
5. Бот-неты. Принцип функционирования.
6. Бот-неты. Методы обнаружения
7. Классификация антивирусных средств.
8. Сигнатурный и эвристический анализ
9. Несанкционированное копирование программ как тип НСД
10. Юридические аспекты несанкционированного копирования программ.
11. Общее понятие защиты от копирования.
12. Проблема защиты отчуждаемых компонентов ПЭВМ.
13. Методы защиты информации на отчуждаемых носителях.
14. Создание посекторных образов НЖМД.
15. Безвозвратное удаление данных. Принципы и алгоритмы.
16. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ
17. СОВ и СОА, отличия в функциях.
18. Основные архитектуры СОВ
19. Использование сетевых снифферов в качестве СОВ
20. Аппаратный компонент СОВ.
21. Программный компонент СОВ
22. Модели системы обнаружения вторжений,
23. Классификация систем обнаружения вторжений.

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК.02.02 Криптографические средства защиты информации.

1. Элементы теории множеств.
2. Группы, кольца, поля.
3. Делимость чисел.
4. Простые и составные числа.
5. Основная теорема арифметики.
6. Алгоритмы факторизации. Факторизация Ферма.
7. Метод Полларда.
8. Алгоритмы дискретного логарифмирования.

9. Метод Полларда.
10. Метод Шорра.
11. Арифметические операции над большими числами.
12. Эллиптические кривые и их приложения в криптографии.
13. Классификация основных методов криптографической защиты.
14. Методы симметричного шифрования
15. Шифры замены.
16. Простая замена,
17. Многоалфавитная подстановка,
18. Пропорциональный шифр
19. Методы перестановки.
20. Табличная перестановка,
21. Маршрутная перестановка
22. Гаммирование.
23. Гаммирование с конечной и бесконечной гаммами
24. Основные методы криптоанализа.
25. Криптографические атаки.
26. Криптографическая стойкость.
27. Абсолютно стойкие криптосистемы.
28. Принципы Киркхоффа
29. Перспективные направления криптоанализа.
30. Основные принципы поточного шифрования.

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по ПМ 02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

1. Предмет и задачи программно-аппаратной защиты информации
2. Основные понятия программно-аппаратной защиты информации
3. Классификация методов и средств программно-аппаратной защиты информации
4. Автоматизация процесса обработки информации
5. Понятие автоматизированной системы.
6. Особенности автоматизированных систем в защищенном исполнении.
7. Основные виды АС в защищенном исполнении.
8. Методы создания безопасных систем
9. Методология проектирования гарантированно защищенных КС
10. Дискреционные модели.
11. Мандатные модели
12. Способы воздействия на информацию.
13. Причины и условия дестабилизирующего воздействия на информацию
14. Понятие несанкционированного доступа к информации
15. Основные подходы к защите информации от НСД
16. Организация доступа к файлам

17. Контроль доступа и разграничение доступа
18. Иерархический доступ к файлам.
19. Фиксация доступа к файлам
20. Доступ к данным со стороны процесса
21. Особенности защиты данных от изменения.
22. Шифрование.
23. Работа автономной АС в защищенном режиме
24. Алгоритм загрузки ОС.
25. Системы типа Электронный замок.
26. Понятие АМДЗ (доверенная загрузка)
27. Изучение и обратное проектирование ПО
28. Способы изучения ПО: статическое и динамическое изучение
29. Задачи защиты от изучения и способы их решения
30. Защита от отладки.
31. Защита от дизассемблирования
32. Защита от трассировки по прерываниям.
33. Вредоносное программное обеспечение как особый вид разрушающих воздействий
34. Классификация вредоносного программного обеспечения.
35. Схема заражения.
36. Средства нейтрализации вредоносного ПО.
37. Бот-нет. Принцип функционирования.
38. Бот-нет. Методы обнаружения
39. Классификация антивирусных средств.
40. Сигнатурный и эвристический анализ
41. Несанкционированное копирование программ как тип НСД
42. Юридические аспекты несанкционированного копирования программ.
43. Общее понятие защиты от копирования.
44. Проблема защиты отчуждаемых компонентов ПЭВМ.
45. Методы защиты информации на отчуждаемых носителях.
46. Создание посекторных образов НЖМД.
47. Безвозвратное удаление данных. Принципы и алгоритмы.
48. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ
49. СОВ и СОА, отличия в функциях.
50. Основные архитектуры СОВ
51. Использование сетевых снифферов в качестве СОВ
52. Аппаратный компонент СОВ.
53. Программный компонент СОВ
54. Модели системы обнаружения вторжений,
55. Классификация систем обнаружения вторжений.
56. Группы, кольца, поля.
57. Делимость чисел.
58. Простые и составные числа.
59. Основная теорема арифметики.

60. Алгоритмы факторизации. Факторизация Ферма.
61. Метод Полларда.
62. Алгоритмы дискретного логарифмирования.
63. Метод Полларда.
64. Метод Шорра.
65. Арифметические операции над большими числами.
66. Эллиптические кривые и их приложения в криптографии.
67. Классификация основных методов криптографической защиты.
68. Методы симметричного шифрования
69. Шифры замены.
70. Простая замена,
71. Многоалфавитная подстановка,
72. Пропорциональный шифр
73. Методы перестановки.
74. Табличная перестановка,
75. Маршрутная перестановка
76. Гаммирование.
77. Гаммирование с конечной и бесконечной гаммами
78. Основные методы криптоанализа.
79. Криптографические атаки.
80. Криптографическая стойкость.
81. Абсолютно стойкие криптосистемы.
82. Принципы Киркхоффа
83. Перспективные направления криптоанализа,
84. квантовый криптоанализ.
85. Основные принципы поточного шифрования.

ФГАОУ ВО «Тюменский государственный университет»
Школа компьютерных наук
Кафедра Информационной безопасности

УТВЕРЖДЕНО
Заместителем директора школы,
А.В. Сапожниковой
РАЗРАБОТЧИК
А.А. Оленников

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Рабочая программа профессионального модуля

включая междисциплинарные курсы (далее – МДК):

МДК.03.01 ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

**МДК.03.02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ
ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ**

Специальность: 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Форма обучения: Очная

язык реализации: Русский

Тюмень, 2024

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
<p>ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5.</p>	<p>31 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;</p> <p>32 номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров</p>	<p>У1 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;</p> <p>У2 применять технические средства для криптографической защиты информации конфиденциального характера;</p> <p>У3 применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;</p>	<p>Н1 Применения средств охранной сигнализации, охранного телевидения и систем контроля и управления доступом;</p> <p>Н2 применения технических средств для криптографической защиты информации аппаратных средств;</p> <p>Н3 применения технических средств для уничтожения информации и носителей информации.</p>

	<p>фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;</p> <p>33 основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;</p> <p>34 основные способы физической защиты объектов информатизации;</p> <p>35 методики инструментального контроля эффективности защиты информации, обрабатываемой</p>	<p>У4 применять инженерно-технические средства физической защиты объектов информатизации.</p>	
--	--	---	--

	<p>средствами вычислительной техники на объектах информатизации; 36 номенклатуру применяемых средств защиты информации от несанкционированн ой утечки по техническим каналам и физической защиты объектов информатизации.</p>		
--	---	--	--

2. Структура и содержание профессионального модуля

Рабочая программа профессионального модуля ПМ.03 «Защита информации техническими средствами» является обязательной частью образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по очной форме обучения.

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и учебным планом образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Цель профессионального модуля состоит в освоении знаний, приобретении умений, получении практического опыта и формировании компетенций в области

защиты информации в автоматизированных системах программными и программно-аппаратными средствами.

2.1. Структура профессионального модуля

Наименования разделов профессионального модуля (МДК)	Семестр	Всего (ак.ч.)	В т.ч. в форме практической подготовки	Учебные занятия по МДК (всего ак.ч.)	Самостоятельная работа по МДК	Курсовые работы (проекты)	Форма промежуточной аттестации
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>
МДК.03.01 Техническая защита информации	5	116	–	76	34	–	Экзамен
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	5	144	–	76	66	–	дифференцированный зачет
Консультации			6				
Экзамен по модулю	5	6					Экзамен
Итого по ПМ:		266	–	152	100	–	Экзамен по модулю

2.2. Тематический план и содержание профессионального модуля

Содержание учебного материала	Вид учебной деятельности (ак.ч.)					
	Урок	Лекция	Практическое занятие (Семинар)	Лабораторное / Практическое занятие по	Выполнение курсового проекта (работы)	Самостоятельная работа

МДК.03.01 Техническая защита информации.						
Семестр 5						
Раздел 1. Концепция инженерно-технической защиты информации.						
Тема 1.1. Предмет и задачи технической защиты информации.		2		2		
Тема 1.2. Общие положения защиты информации техническими средствами.		2		2		4
Раздел 2. Теоретические основы инженерно-технической защиты информации.						
Тема 2.1. Информация как предмет защиты.		2		2		4
Тема 2.2. Технические каналы утечки информации.		2		2		4
Тема 2.3. Методы и средства технической разведки.		2		2		
Раздел 3. Физические основы технической защиты информации.						
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.		2		2		4
Тема 3.2. Физические процессы при подавлении опасных сигналов.		2		2		4
Раздел 4. Системы защиты от утечки информации.						
Тема 4.1. Системы защиты от утечки информации по акустическому каналу.		2		2		
Тема 4.2. Системы защиты от утечки информации по проводному каналу.		2		2		
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу.		2		2		4
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу.		2		2		
Тема 4.5. Системы защиты от утечки информации по телефонному каналу.		2		2		4
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу.		2		2		6
Тема 4.7. Системы защиты от утечки информации по оптическому каналу.		4		4		
Раздел 5. Применение и эксплуатация технических средств защиты информации.						
Тема 5.1. Применение технических средств защиты информации.		4		4		
Тема 5.2. Эксплуатация технических средств защиты информации.		4		4		
Консультации		2				

Промежуточная аттестация	экзамен				
Всего		38		38	34
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.					
Семестр 5					
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты.					
Тема 1.1. Цели и задачи физической защиты объектов информатизации.		4		4	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты.		4		4	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты.					
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты.		4		4	10
Тема 2.2. Система контроля и управления доступом.		6		6	10
Тема 2.3. Система телевизионного наблюдения.		4		4	12
Тема 2.4. Система сбора, обработки, отображения и документирования информации.					
Тема 2.5 Система воздействия.		4		4	8
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты.					
Тема 3.1 Применение инженерно-технических средств физической защиты.		6		6	14
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты.		6		6	12
Консультации	2				
Промежуточная аттестация	дифференцированный зачет				
Всего		38		38	66
Всего по модулю		76		76	100

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК.03.01 «Техническая защита информации» в 5 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.03.02 «Инженерно-технические средства физической защиты объектов информатизации» в 5 семестре предусмотрен дифференцированный зачет. Дифференцированный зачет является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в

полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

4.1.1. Основная литература:

МДК.03.01 Техническая защита информации

1. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва ; Вологда : Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2169702> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543631> (дата обращения: 09.09.2024).

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/557735> (дата обращения: 09.09.2024).

2. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/555949> (дата обращения: 09.09.2024).

4.1.2. Дополнительная литература:

МДК.03.01 Техническая защита информации

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2130242> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

2. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1898839> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

1. Цифровые технологии в учебном процессе : учебник (с электронными приложениями) / С. В. Алексахин, В. И. Блинов, И. С. Сергеев, В. А. Тармин. - Москва : РИОР : ИНФРА-М, 2023. - 311 с. - DOI: <https://doi.org/10.29039/01922-1>. - ISBN 978-5-369-01922-1. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2019008> (дата обращения: 09.09.2024).

2. Гвоздева, В. А. Информатика, автоматизированные информационные технологии и системы : учебник / В.А. Гвоздева. — Москва : ИД «ФОРУМ» :

ИНФРА-М, 2020. — 542 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0856-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1067007> (дата обращения: 09.09.2024). – Режим доступа: по подписке.

4.1.3. Современные профессиональные базы данных и информационные справочные системы:

- Научная электронная библиотека eLIBRARY.RU;
- Springer;
- JSTOR;
- База данных ООО «ИВИС»;
- База данных IPR Books;
- Образовательная платформа Юрайт.

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

LibreOffice, платформы: Яндекс. Мессенджер, Яндекс.Телемост.

4.3. Материально-техническое обеспечение реализации дисциплины:

Кабинет информационных технологий, программирования и баз данных.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран.

Программное обеспечение: платформа Яндекс 360 (телемост, мессенджер), операционная система Альт Образование, офисный пакет Libre Office (Writer, Impress, Draw, Base, Calc, Math), сетевые браузеры Chromium, Яндекс Браузер. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения групповых и индивидуальных консультаций.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная.

Технические средства обучения: персональный компьютер, проектор, звуковой усилитель, колонки, экран.

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения промежуточной и итоговой аттестации.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для организации самостоятельной и воспитательной работы.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного

производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ МДК.03.01 ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ МДК.03.02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ Открытая часть

1. Система оценивания

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК.03.01 «Техническая защита информации» в 5 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен

выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК.03.02 «Инженерно-технические средства физической защиты объектов информатизации» в 5 семестре предусмотрен дифференцированный зачет. Дифференцированный зачет является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы (виды и количество)	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.03.01 Техническая защита информации			
Текущий контроль успеваемости			
Тема 1.1. Предмет и задачи технической защиты информации.	Лабораторная работа	ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;	5 баллов
Тема 1.2. Общие положения защиты информации техническими средствами.	Лабораторная работа	ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;	5 баллов
Тема 2.1. Информация как предмет защиты.	Лабораторная работа	ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;	5 баллов
Тема 2.2. Технические каналы утечки информации.	Лабораторная работа	ОК 04. Эффективно взаимодействовать и	5 баллов
Тема 2.3. Методы и средства технической разведки.	Лабораторная работа		5 баллов
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.	Лабораторная работа		5 баллов
Тема 3.2. Физические процессы при подавлении опасных сигналов.	Лабораторная работа		5 баллов
Тема 4.1. Системы защиты от утечки информации по акустическому каналу.	Лабораторная работа		5 баллов
Тема 4.2. Системы защиты от утечки информации по проводному каналу.	Лабораторная работа		5 баллов

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу.	Лабораторная работа	работать в коллективе и команде; ОК 05. Осуществлять устную и письменную коммуникацию на	5 баллов
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу.	Лабораторная работа	государственном языке Российской Федерации с учетом особенностей социального и	5 баллов
Тема 4.5. Системы защиты от утечки информации по телефонному каналу.	Лабораторная работа	культурного контекста; ОК 06. Проявлять гражданско-	5 баллов
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу.	Лабораторная работа	патриотическую позицию, демонстрировать осознанное поведение на основе	5 баллов
Тема 4.7. Системы защиты от утечки информации по оптическому каналу.	Лабораторная работа	традиционных российских духовно-нравственных ценностей, в том числе с	5 баллов
Тема 5.1. Применение технических средств защиты информации.	Лабораторная работа	с учетом гармонизации межнациональных и	5 баллов
Тема 5.2. Эксплуатация технических средств защиты информации.	Лабораторная работа	межрелигиозных отношений, применять стандарты антикоррупционного поведения; ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в	5 баллов
		чрезвычайных ситуациях;	

		<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;</p> <p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.</p> <p>ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.</p> <p>ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.</p> <p>ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации</p>	
--	--	---	--

		ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	
Промежуточная аттестация обучающихся			
Экзамен	5 семестр	ОК 01 – ОК 09, ПК 3.1 – ПК 3.4	
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации			
Текущий контроль успеваемости			
Тема 1.1. Математические основы криптографии.	Практическая работа	ОК 01. Выбирать способы решения задач	5 баллов
Тема 2.1. Методы криптографического защиты информации.	Практическая работа	профессиональной деятельности применительно к	5 баллов
Тема 2.2. Криптоанализ.	Практическая работа	различным контекстам;	5 баллов
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел.	Практическая работа	ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и	5 баллов
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Практическая работа	информационные технологии для выполнения задач	5 баллов
Тема 3.2. Симметричные системы шифрования.	Практическая работа	профессиональной деятельности;	5 баллов
Тема 3.3. Асимметричные системы шифрования.	Практическая работа	ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и	5 баллов
Тема 3.4. Аутентификация данных. Электронная подпись.	Практическая работа		5 баллов
Тема 3.5. Алгоритмы обмена ключей и	Практическая работа		5 баллов

протоколы аутентификации.		финансовой грамотности в	
Тема 3.6. Криптозащита информации в сетях передачи данных.	Практическая работа	различных жизненных ситуациях; ОК 04. Эффективно взаимодействовать и	5 баллов
Тема 3.7. Защита информации в электронных платежных системах.	Практическая работа	работать в коллективе и команде; ОК 05. Осуществлять устную и письменную	5 баллов
Тема 3.8. Компьютерная стеганография.	Практическая работа	коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста; ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения; ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого	5 баллов

		производства, 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. Пользоваться профессиональной документацией на государственном и иностранном языках. ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	
Промежуточная аттестация обучающихся			
Дифференцированный зачет	5 семестр	ОК 01 – ОК 09 ПК 3.5	
Экзамен по модулю	5 семестр	ОК 01 – ОК 09 ПК 3.1 – ПК 3.5	

3. Типовые оценочные материалы

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК.03.01 Техническая защита информации.

1. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.

2. Системный подход при решении задач инженерно-технической защиты информации.
3. Основные параметры системы защиты информации.
4. Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации.
5. Классификация способов и средств защиты информации.
6. Особенности информации как предмета защиты. Свойства информации.
7. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале.
8. Источники опасных сигналов. Основные и вспомогательные технические средства и системы.
9. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.
10. Понятие и особенности утечки информации. Структура канала утечки информации.
11. Классификация существующих физических полей и технических каналов утечки информации.
12. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.
13. Классификация технических средств разведки. Методы и средства технической разведки.
14. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.
15. Физические основы побочных электромагнитных излучений и наводок.
16. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств.
17. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.
18. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей
19. Технические средства акустической разведки.
20. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами.
21. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
22. Электронные стетоскопы. Лазерные системы подслушивания.
23. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу.

24. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.
25. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.
26. Использование микрофона телефонного аппарата при положенной телефонной трубке.
27. Утечка информации по сотовым цепям связи.
28. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.
29. Технические средства для уничтожения информации и носителей информации, порядок применения.
30. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.

1. Характеристики потенциально опасных объектов.
2. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты.
3. Категорирование объектов информатизации.
4. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.
5. Особенности задач охраны различных типов объектов.
6. Общие принципы обеспечения безопасности объектов.
7. Жизненный цикл системы физической защиты.
8. Принципы построения интегрированных систем охраны.
9. Классификация и состав интегрированных систем охраны.
10. Требования к инженерным средствам физической защиты.
11. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации
12. Информационные основы построения системы охранной сигнализации.
13. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.
14. Периметровые средства обнаружения: назначение, устройство, принцип действия.
15. Объектовые средства обнаружения: назначение, устройство, принцип действия.
16. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД.
17. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД.
18. Основы построения и принципы функционирования СКУД.

19. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.
20. Обнаружение металлических предметов и радиоактивных веществ.
21. Аналоговые и цифровые системы видеонаблюдения. Назначение систем телевизионного наблюдения.
22. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи.
23. Поворотные системы. Инфракрасные осветители. Детекторы движения
24. Классификация системы сбора и обработки информации.
25. Схема функционирования системы сбора и обработки информации.
26. Варианты структур построения системы сбора и обработки информации.
27. Устройства отображения и документирования информации.
28. Периметровые и объектовые средства обнаружения, порядок применения.
29. Работа с периферийным оборудованием системы контроля и управления доступом.
30. Особенности организации пропускного режима на КПП.

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по ПМ 03 «Защита информации техническими средствами»

1. Предмет и задачи технической защиты информации.
2. Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований
3. Классификация технических средств разведки. Методы и средства технической разведки.
4. Расшифровать шифр текст, зашифрованный методом вертикальной перестановки: «оамноднрнзотнциаииооенрфибскиаопт». Ключом является слово «заслон».
5. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.
6. Электронные стетоскопы. Лазерные системы подслушивания
7. Телевизионные системы наблюдения.
8. Расшифровать шифртекст, зашифрованный методом Плейфера: «лбгтньефгжтвгцсешйоажгиттвияль». Ключом является слово «агентство».
9. Технические средства для уничтожения информации и носителей информации, порядок применения.
10. Физические основы побочных электромагнитных излучений и наводок.
11. Акустоэлектрические преобразования.
12. Задачи и требования к способам и средствам защиты информации техническими средствами.
13. Расшифровать шифртекст «474407», зашифрованный методом RSA. Ключ задан следующими параметрами: $p=17$, $q=31$, $e=7$.

14. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале.
15. Этапы эксплуатации технических средств защиты информации.
16. Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.
17. Расшифровать шифртекст, зашифрованный методом Вижинера. Ключом является слово «энигма».
18. Системный подход при решении задач инженерно-технической защиты информации.
19. Источники опасных сигналов. Основные и вспомогательные технические средства и системы.
20. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.
21. Расшифровать текст, зашифрованный двойным квадратом Уитстона.
22. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
23. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.
24. Понятие и особенности утечки информации. Структура канала утечки информации
25. Устройства отображения и документирования информации.

ФГАОУ ВО «Тюменский государственный университет»
Школа компьютерных наук
Кафедра Информационной безопасности

УТВЕРЖДЕНО
Заместителем директора школы,
А.В. Сапожниковой
РАЗРАБОТЧИК
А.А. Оленников

**ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ
ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ**

Рабочая программа профессионального модуля
включая междисциплинарный курс (далее – МДК):

**МДК.04.01 ВЫПОЛНЕНИЕ РАБОТ ПО РАБОЧЕЙ ПРОФЕССИИ
«ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И
ВЫЧИСЛИТЕЛЬНЫХ МАШИН»**

Специальность: 10.02.05 Обеспечение информационной безопасности
автоматизированных систем
Форма обучения: Очная
язык реализации: Русский

Тюмень, 2024

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ПК 4.1, ПК 4.2, ПК 4.3, ПК 4.4.	31 требования техники безопасности при работе с вычислительной техникой;	У1 выполнять требования техники безопасности при работе с вычислительно техникой;	Н1 выполнения требований техники безопасности при работе с вычислительной техникой;
	32 основные принципы устройства и работы компьютерных систем и периферийных устройств;	У2 производить подключение блоков персонального компьютера и периферийны устройств;	Н2 подключения блоков персонального компьютера и периферийны устройств;
	33 классификацию и назначение компьютерных сетей;	У3 производить установку и замену расходных материалов для периферийны устройств и компьютерной оргтехники;	Н3 установки и замены расходных материалов для периферийны устройств;
	34 виды носителей информации;	У4 диагностировать простейшие неисправности персонального компьютер периферийного оборудования и	Н4 диагностики простейших неисправностей персонального компьютера.
	35 программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета;		
	36 основные средства защиты от		

	<p>вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.</p>	<p>компьютерной оргтехники;</p> <p>У5 выполнять установку и системного и прикладного программного обеспечения;</p> <p>У6 создавать и управлять содержимым документов с помощью текстовых процессоров;</p> <p>У7 создавать и управлять содержимым электронных таблиц с помощью редактора таблиц;</p> <p>У8 создавать и управлять содержимым презентаций с помощью редактора презентаций;</p> <p>У9 использовать мультимедиа проектор для</p>	
--	---	---	--

		<p>демонстрации презентаций;</p> <p>У10 вводить, редактировать и удалять записи в базе данных;</p> <p>У11 эффективно пользоваться запросами базы данных;</p> <p>У12 создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;</p> <p>У13 производить сканирование документов и их распознавание;</p> <p>У14 производить распечатку, копирование и тиражирование документов на принтере и других устройствах;</p> <p>У15 управлять файлами данных на</p>	
--	--	---	--

		<p>ЛОКАЛЬНЫХ СЪЕМНЫХ запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете;</p> <p>У16 осуществлять навигацию по Веб- ресурсам Интернета с помощью браузера;</p> <p>У17 осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов;</p> <p>У18 осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;</p> <p>У19 осуществлять резервное копирование и восстановление данных.</p>	
--	--	--	--

2. Структура и содержание профессионального модуля

Рабочая программа профессионального модуля ПМ.04 «Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих» является обязательной частью образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по очной форме обучения.

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и учебным планом образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Цель профессионального модуля состоит в освоении знаний, приобретении умений, получении практического опыта и формировании компетенций в области защиты информации в автоматизированных системах программными и программно-аппаратными средствами.

2.1. Структура профессионального модуля

Наименования разделов профессионального модуля (МДК)	Семестр	Всего (ак.ч.)	В т.ч. в форме практической подготовки	Учебные занятия по МДК (всего ак.ч.)	Самостоятельная работа по МДК	Курсовые работы (проекты)	Форма промежуточной аттестации
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>
МДК.04.01 Выполнение работ по рабочей профессии «оператор электронно-вычислительных и вычислительных машин»	2	102	–	20	80	–	Дифференцированный зачет
Консультации					4		

Экзамен по модулю	2	6					Экзаме н
Итого по ПМ:	2	108	–	20	80	–	Экзаме н по модул ю

2.2. Тематический план и содержание профессионального модуля

Содержание учебного материала	Вид учебной деятельности (ак.ч.)					
	Урок	Лекция	Практическое занятие (Семинар)	Лабораторное / Практическое занятие по	Выполнение курсового проекта (работы)	Самостоятельная работа
МДК.04.01 Выполнение работ по рабочей профессии «оператор электронно-вычислительных и вычислительных машин».						
Семестр 2						
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения.						
Тема 1.1. Работа с устройствами компьютерной системы.			2			4
Тема 1.2. Работа с программным обеспечением компьютерной системы.			2			4
Тема 1.3. Диагностика неисправностей системы, ведение документации.			2			8
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах.						
Тема 2.1. Работа в текстовом процессоре.			2			8
Тема 2.2. Работа в редакторе электронных таблиц.			2			8
Тема 2.3. Работа в программе подготовки и просмотра презентаций.			2			6

Тема 2.4. Работа в системе управления базами данных.			2			10
Тема 2.5. Работа в графических редакторах.			2			10
Раздел 3. Использование ресурсов технологий и сервисов Интернета.						
Тема 3.1. Работа с ресурсами Интернета.			2			10
Раздел 4. Обеспечение защиты информации в компьютерной системе.						
Тема 4.1. Защита информации при работе с офисными приложениями.			2			20
Консультации	2					
Промежуточная аттестация	дифференцированный зачет					
Всего			20			80
Всего по модулю			20			80

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК.04.01 «Выполнение работ по рабочей профессии «оператор электронно-вычислительных и вычислительных машин» во 2 семестре предусмотрен зачет с оценкой. Зачет является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из

билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

4.1.1. Основная литература:

МДК.04.01 Выполнение работ по рабочей профессии «оператор электронно-вычислительных и вычислительных машин».

1. 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 ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст

: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512861> (дата обращения: 09.09.2024).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/557735> (дата обращения: 09.09.2024).

3. Рассолов, И. М. Информационное право : учебник для среднего профессионального образования / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 427 с. — (Профессиональное образование). — ISBN 978-5-534-18147-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/545131> (дата обращения: 09.09.2024).

4. 3D-моделирование в дизайне и технологии художественной обработки материалов : учебное пособие / В. А. Кукушкина, Е. А. Кантарюк, Л. С. Абдуллах, Ю. А. Бордюгова. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2024. — 53 с. — ISBN 978-5-00175-252-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/140682.html> (дата обращения: 09.09.2024). — Режим доступа: для авторизир. пользователей.

4.1.2. Дополнительная литература:

МДК.04.01 Выполнение работ по рабочей профессии «оператор электронно-вычислительных и вычислительных машин».

1. Голицына, О. Л. Основы алгоритмизации и программирования : учебное пособие / О. Л. Голицына, И.И. Попов. -4-е изд., испр. и доп. -Москва :ФОРУМ : ИНФРА-М, 2021. -431 с. -(Среднее профессиональное образование). - ISBN 978-5-00091-570-7. -Текст : электронный // ЭБС ZNANIUM.COM : сайт. - URL: <https://znanium.com/catalog/product/1150328> (дата обращения: 03.09.2020).

2. Кудрина, Е. В. Основы алгоритмизации и программирования на языке C# : учебное пособие для среднего профессионального образования / Е. В.

Кудрина, М. В. Огнева. — Москва : Издательство Юрайт, 2023. — 322 с. — (Профессиональное образование). — ISBN 978-5-534-10772-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/517324> (дата обращения: 09.09.2024).

3. Огнева, М. В. Программирование на языке C++: практический курс : учебное пособие для среднего профессионального образования / М. В. Огнева, Е. В. Кудрина. — Москва : Издательство Юрайт, 2023. — 335 с. — (Профессиональное образование). — ISBN 978-5-534-05780-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/515206>

4. Трофимов, В. В. Основы алгоритмизации и программирования : учебник для среднего профессионального образования / В. В. Трофимов, Т. А. Павловская ; под редакцией В. В. Трофимова. — 4-е изд. — Москва : Издательство Юрайт, 2023. — 119 с. — (Профессиональное образование). — ISBN 978-5-534-17498-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/533200>

4.1.3. Современные профессиональные базы данных и информационные справочные системы:

- Научная электронная библиотека eLIBRARY.RU;
- Springer;
- JSTOR;
- База данных ООО «ИВИС»;
- База данных IPR Books;
- Образовательная платформа Юрайт.

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

LibreOffice, платформы: Яндекс. Мессенджер, Яндекс.Телемост.

4.3. Материально-техническое обеспечение реализации дисциплины:

Кабинет информационных технологий, программирования и баз данных.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран.

Программное обеспечение: платформа Яндекс 360 (телемост, мессенджер), операционная система Альт Образование, офисный пакет Libre Office (Writer, Impress, Draw, Base, Calc, Math), сетевые браузеры Chromium, Яндекс Браузер. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения групповых и индивидуальных консультаций.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная.

Технические средства обучения: персональный компьютер, проектор, звуковой усилитель, колонки, экран.

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения промежуточной и итоговой аттестации.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для организации самостоятельной и воспитательной работы.

Основное оборудование: столы, стулья, рабочее место преподавателя, доска аудиторная. Технические средства обучения: персональные компьютеры, проектор, звуковой усилитель, колонки, экран

Программное обеспечение: установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ
МОДУЛЮ
ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ
ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ**

**МДК.04.01 ВЫПОЛНЕНИЕ РАБОТ ПО РАБОЧЕЙ ПРОФЕССИИ
«ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И
ВЫЧИСЛИТЕЛЬНЫХ МАШИН»**

Открытая часть

1. Система оценивания

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК.04.01 «Выполнение работ по рабочей профессии «оператор электронно-вычислительных и вычислительных машин» во 2 семестре предусмотрен дифференцированный зачет. Дифференцированный зачет является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами

специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы (виды и количество)	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.04.01 Выполнение работ по рабочей профессии "Оператор электронно-вычислительных и вычислительных машин"			
Текущий контроль успеваемости			
Тема 1.1. Работа с устройствами компьютерной системы.	Практическая работа	ОК 01. Выбирать способы решения задач профессиональной деятельности	5 баллов
Тема 1.2. Работа с программным обеспечением компьютерной системы.	Практическая работа	применительно к различным контекстам; ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и	5 баллов
Тема 1.3. Диагностика неисправностей системы, ведение документации.	Практическая работа	информационные технологии для выполнения задач профессиональной деятельности;	5 баллов
Тема 2.1. Работа в текстовом процессоре.	Практическая работа	ОК 03. Планировать и реализовывать собственное профессиональное и	5 баллов
Тема 2.2. Работа в редакторе электронных таблиц.	Практическая работа		5 баллов
Тема 2.3. Работа в программе подготовки и просмотра презентаций.	Практическая работа		15 баллов

Тема 2.4. Работа в системе управления базами данных.	Практическая работа	личностное развитие, предпринимательскую деятельность в	15 баллов
Тема 2.5. Работа в графических редакторах.	Практическая работа	профессиональной сфере, использовать знания по правовой и	5 баллов
Тема 3.1. Работа с ресурсами Интернета.	Практическая работа	финансовой грамотности в	5 баллов
Тема 4.1. Защита информации при работе с офисными приложениями.	Практическая работа	различных жизненных ситуациях; ОК 04. Эффективно взаимодействовать и работать в коллективе и команде; ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста; ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения; ОК 07. Содействовать сохранению окружающей среды,	5 баллов

		<p>ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;</p> <p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;</p> <p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.</p> <p>ПК 4.1. Устанавливать программные, программно-аппаратные (в том числе криптографические) и технические средства и систем защиты средств связи сетей электросвязи от несанкционированного доступа.</p> <p>ПК 4.2. Обеспечивать бесперебойную работу средств связи сетей электросвязи, а также программных, программно-</p>	
--	--	---	--

		<p>аппаратных (в том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа, средств для поиска признаков компьютерных атак в сетях электросвязи.</p> <p>ПК 4.3. Проводить техническое обслуживание средств связи сетей электросвязи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от несанкционированного доступа, средств для поиска признаков компьютерных атак в сетях электросвязи.</p> <p>ПК 4.4. Проводить техническое обслуживание средств защиты информации прикладного и системного программного обеспечения.</p>	
Промежуточная аттестация обучающихся			
Дифференцированный зачет	2 семестр	ОК 01 – ОК 09, ПК 4.1 – ПК 4.4	
Экзамен по модулю	2 семестр	ОК 01 – ОК 09, ПК 4.1 – ПК 4.4	

3. Типовые оценочные материалы

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по МДК.04.01 Выполнение работ по рабочей профессии "Оператор электронно-вычислительных и вычислительных машин".

1. Эргономика рабочего места
2. Общие сведения об электронно – вычислительных машинах
3. Роль вычислительной техники в автоматизированных системах управления
4. Дайте определение технологического процесса обработки отраслевой информации.
5. Перечислите факторы характеризующие технологического процесса обработки отраслевой информации.
6. Дайте определение стандартизации технологического процесса обработки информации.
7. Назовите этапы технологического процесса обработки отраслевой информации.
8. Охарактеризуйте каждый этап технологического процесса обработки отраслевой информации.
9. Понятие информации, информационных технологий. Классификации информационных технологий.
10. Основные методы и средства обработки, хранения, передачи и накопления информации. Системы счисления.
11. Назначение и основные характеристики системного блока ЭВМ
12. Назначение и основные характеристики флэш – памяти, монитора, мыши, клавиатуры, принтера, графопостроителя, сканера, модема.
13. Технические компоненты ЭВМ
14. Назначение и принципы использования системного программного обеспечения
15. Назначение и принципы использования прикладного программного обеспечения
16. Введение в компьютерные сети. Каналы передачи данных.
17. Классификации компьютерных сетей
18. Топологии локальных компьютерных сетей
19. Принципы построения сети Интернет
20. Глобальная компьютерная сеть
21. Методы и средства защиты информации в компьютерных системах.
Информационная безопасность и ее компоненты
22. Методы и средства защиты в компьютерных системах
23. Основные приемы работы, элементы текстового редактора
24. Дополнительные возможности текстового редактора

25. Ввод данных. Форматы данных ячеек. Ввод текста и чисел.
Форматирование ячеек.
26. Создание формул. Ссылки. Табличный процессор OpenOffice Calc
27. Электронные презентации как часть информационных технологий для деловой жизни
28. Понятие о базах данных
29. Типы баз данных. Системы управления базами данных
30. Математические выражения. Графические области. Решение уравнений.

Перечень вопросов для проведения промежуточной аттестации в форме квалификационного экзамена по ПМ 04 «Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих»

1. Эргономика рабочего места
2. Математические выражения. Графические области. Решение уравнений.
3. Основы работы с MathCad
4. Общие сведения об электронно – вычислительных машинах
5. Роль вычислительной техники в автоматизированных системах управления
6. Введение в компьютерные сети. Каналы передачи данных.
7. Построить таблицу истинности для предложенной формулы
8. Дайте определение технологического процесса обработки отраслевой информации.
9. Классификации компьютерных сетей
10. Доказать правильность выражения логической функции через базовую логическую функцию
11. Перечислите факторы характеризующие технологического процесса обработки отраслевой информации.
12. Топологии локальных компьютерных сетей
13. Наберите следующий текст, растянув его на страницу и соблюдая все форматы абзацев и символов: выравнивание (по ширине); левые (1,25 см) и правые отступы (1 см); расстояния между абзацами (1,15); тип (TimesNR), размер (12) и начертание (курсив) шрифтов.
14. Дайте определение стандартизации технологического процесса обработки информации.
15. Принципы построения сети Интернет
16. Создайте документ OpenOffice Writer с вашей краткой автобиографией (Не менее 15 строк: зовут так-то, родился тогда-то, люблю то-то, увлекаюсь тем-то, не нравится то-то и т.п.).
17. Назовите этапы технологического процесса обработки отраслевой информации.
18. Глобальная компьютерная сеть
19. Охарактеризуйте каждый этап технологического процесса обработки отраслевой информации.
20. Методы и средства защиты информации в компьютерных системах.
Информационная безопасность и ее компоненты

21. Понятие информации, информационных технологий. Классификация информационных технологий.
22. Методы и средства защиты в компьютерных системах
23. Основные методы и средства обработки, хранения, передачи и накопления информации. Системы счисления
24. Основные приемы работы, элементы текстового редактора
25. Наберите и отформатируйте текст по образцу, добавьте рамку на страницу.