ФГАОУ ВО «Тюменский государственный университет»
Колледж искусственного интеллекта, креативного мышления и мастерства

УТВЕРЖДЕНО
Заместителем директора
ИИ Колледжа
Дубровиной Т.Л.
РАЗРАБОТЧИКИ
Дубровина Т.Л.
Волегова Е.А.

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

для обучающихся по специальности: 10.02.05 Обеспечение информационной безопасности автоматизированных систем
форма обучения: очная
язык реализации: русский

Тюмень, 2026

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
ПК 2.1; ПК 2.2; ПК 2.3; ПК 2.4; ПК 2.5; ПК 2.6.	З-1 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; З-2 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; З-3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; З-4 основные понятия криптографии и типовых криптографических методов и средств защиты информации; З-5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; З-6 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	У-1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; У-2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; У-3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; У-4 применять программные и программно-аппаратные средства для защиты информации в базах данных; У-5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; У-6 применять математический аппарат для выполнения криптографических преобразований; У-7 использовать типовые программные криптографические средства, в том числе электронную подпись;	Н-1 установки и настройки, программные и программно-аппаратных средств защиты информации; Н-2 настройки средств антивирусной защиты; Н-3 устранения отказов оборудования; Н-4 применения программных и программно-аппаратных средств; Н-5 применения математических аппаратов для выполнения криптографических преобразований.

		У-8 применять средства гарантированного уничтожения информации; У-9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; У-10 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.	

2. Структура и содержание профессионального модуля

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 (всего ак.ч.)	Курсовые работы (проекты)	Экзамен	Дифференцированный зачет
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
МДК.02.01 Программные и программно-аппаратные средства защиты информации	4	105	–	77	4	20	4	–
МДК.02.02 Криптографические средства защиты информации	4	108	–	97	9	–	–	2
Экзамен по модулю	4	4						
Итого по ПМ:		***217***	**–**	***174***	***13***	***20***	***4***	***2***

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 подгруппам	Выполнение курсового проекта (работы)	Самостоятельная работа
МДК.02.01 Программные и программно-аппаратные средства защиты информации.						
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации.						
Содержание						
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации. Стандарты безопасности. Защищенная автоматизированная система		2		6		
Тема 1.2. Дестабилизирующее воздействие на объекты защиты. Принципы программно-аппаратной защиты информации от несанкционированного доступа.		2		6		
Раздел 2. Защита автономных автоматизированных систем.						
Содержание						
Тема 2.1. Основы защиты автономных автоматизированных систем. Защита программ от изучения. Вредоносное программное обеспечение. Защита программ и данных от несанкционированного копирования.		2		8		
Тема 2.2. Защита информации на машинных носителях. Аппаратные средства идентификации и аутентификации пользователей. Системы обнаружения атак и вторжений		2		8		
Раздел 3. Защита информации в локальных сетях.						
Содержание						
Тема 3.1. Основы построения защищенных сетей. Средства организации VPN.		2		8		
Раздел 4. Защита информации в сетях общего доступа.						
Содержание						
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия.		2		8		
Раздел 5. Защита информации в базах данных.						
Содержание						

Тема 5.1. Защита информации в базах данных.		2		8		
Раздел 6. Мониторинг систем защиты.						
Содержание						
Тема 6.1. Мониторинг систем защиты. Изучение мер защиты информации в информационных системах. Изучение современных программно-аппаратных комплексов.		2		8		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы по программно-аппаратным средствам защиты информации.						4
Консультации	**1 ак.ч.**					
Промежуточная аттестация	**4 ак.ч. - *экзамен***					
Всего	**105**	**16**		**60**	**20**	**4**
МДК.02.02 Криптографические средства защиты информации.						
Раздел 1. Математические основы защиты информации.						
Содержание						
Тема 1.1. Математические основы криптографии.		2		6		
Раздел 2. Классическая криптография.						
Содержание						
Тема 2.1. Методы криптографического защиты информации.		2		6		
Тема 2.2. Криптоанализ.		2		6		
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел.		2		6		
Раздел 3. Современная криптография.						
Содержание						
Тема 3.1. Кодирование информации. Компьютеризация шифрования.		2		6		
Тема 3.2. Симметричные системы шифрования.		2		6		
Тема 3.3. Асимметричные системы шифрования.		2		6		
Тема 3.4. Аутентификация данных. Электронная подпись.		2		6		
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации.		2		6		
Тема 3.6. Криптозащита информации в сетях передачи данных.		2		6		
Тема 3.7. Защита информации в электронных платежных системах.		2		6		
Тема 3.8. Компьютерная стеганография.		2		6		
Самостоятельная работа обучающихся.						

Чтение и разбор литературы по криптографической защите информации.						9
Консультации	**1 ак.ч.**					
Промежуточная аттестация	**2 ак.ч. – *дифференцированный зачет***					
Всего	**108**	**24**		**72**		**9**

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся осуществляются с применением оценочных материалов по профессиональному модулю (приложение № 1 - № 2 к рабочей программе профессионального модуля), включающих открытую (доступную к опубликованию) и закрытую (не размещаемую в свободном доступе) части.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

Учебно-методическое и информационное обеспечение реализации профессионального модуля сформировано с учетом требований ФГОС СПО и ПОП СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Для реализации основной образовательной программы подготовки квалифицированных рабочих, служащих по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем библиотечный фонд ИИ Колледжа имеет печатные и электронные образовательные и информационные ресурсы для использования в образовательном процессе.

4.1.1. Основная 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, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561717 (дата обращения: 22.04.2026).

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, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567283 (дата обращения: 22.04.2026).

3. 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: 22.04.2026).

МДК.02.02 Криптографические средства защиты информации

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580668 (дата обращения: 22.04.2026).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-

20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567521 (дата обращения: 22.04.2026).

4.1.2. Дополнительная литература:

МДК.02.01 Программные и программно-аппаратные средства защиты информации

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567521 (дата обращения: 22.04.2026).

МДК.02.02 Криптографические средства защиты информации

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340 (дата обращения: 22.04.2026).

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:

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК 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.

Мультимедийная учебная аудитория для проведения практических занятий оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК 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 групповых и индивидуальных консультаций оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер (ПК). На ПК 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 оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК

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.

Аудитория для организации самостоятельной и воспитательной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры. На ПК 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.

Библиотека, читальный зал, коворкинг с выходом в интернет.

Приложение № 1
к рабочей программе
профессионального модуля

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Открытая часть

1. Система оценивания

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

Промежуточная аттестация по МДК.02.01 в соответствии с учебным планом предусмотрена в форме экзамена, который проводится в традиционной форме по билетам.

Промежуточная аттестация по МДК.02.02 в соответствии с учебным планом предусмотрена в форме дифференцированного зачета, который проводится в традиционной форме по билетам.

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. Стандарты безопасности. Защищенная автоматизированная система	Лабораторная работа №1	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 2.5. Уничтожать информацию и носители информации с использованием	Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №1 5 баллов
Тема 1.2. Дестабилизирующее воздействие на объекты защиты. Принципы программно-аппаратной защиты информации от несанкционированного доступа.	Лабораторная работа №2		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №2 5 баллов
Тема 2.1. Основы защиты автономных автоматизированных систем. Защита программ от изучения. Вредоносное программное	Лабораторная работа №3		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных

обеспечение. Защита программ и данных от несанкционированного копирования.		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.	занятиях. Экспертная оценка выполнения лабораторной работы №3 5 баллов
Тема 2.2. Защита информации на машинных носителях. Аппаратные средства идентификации и аутентификации пользователей. Системы обнаружения атак и вторжений	Лабораторная работа №4		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №4 5 баллов
Тема 3.1. Основы построения защищенных сетей. Средства организации VPN.	Лабораторная работа №5		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №5 5 баллов
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	Лабораторная работа №6		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №6 5 баллов
Тема 5.1. Защита информации в базах данных	Лабораторная работа №7		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №7 5 баллов
Тема 6.1. Мониторинг систем защиты. Изучение мер защиты информации в информационных	Лабораторная работа №8		Экспертное наблюдение и оценивание ЗУН на теоретических и

системах. Изучение современных программно-аппаратных комплексов.			лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №8 5 баллов
Промежуточная аттестация обучающихся			
Экзамен, 4 семестр	Вопросы к экзамену – 23 вопроса	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	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.

МДК.02.02 Криптографические средства защиты информации			
Текущий контроль успеваемости			
Тема 1.1. Математические основы криптографии.	Лабораторная работа №1	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №1 5 баллов
Тема 2.1. Методы криптографического защиты информации.	Лабораторная работа №2		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №2 5 баллов
Тема 2.2. Криптоанализ.	Лабораторная работа №3		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №3 5 баллов
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел.	Лабораторная работа №4		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №4 5 баллов
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Лабораторная работа №5		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка

			выполнения лабораторной работы №5 5 баллов
Тема 3.2. Симметричные системы шифрования	Лабораторная работа №6		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №6 5 баллов
Тема 3.3. Асимметричные системы шифрования	Лабораторная работа №7		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №7 5 баллов
Тема 3.4. Аутентификация данных. Электронная подпись.	Лабораторная работа №8		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №8 5 баллов
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации.	Лабораторная работа №9		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №9 5 баллов
Тема 3.6. Криптозащита информации в сетях передачи данных.	Лабораторная работа №10		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных

			занятиях. Экспертная оценка выполнения лабораторной работы №10 5 баллов
Тема 3.7. Защита информации в электронных платежных системах.	Лабораторная работа №11		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №11 5 баллов
Тема 3.8. Компьютерная стеганография.	Лабораторная работа №12		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №12 5 баллов

Промежуточная аттестация обучающихся			
Дифференцированный зачет, 4 семестр	Вопросы к экзамену – 30 вопросов	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	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.

3. Типовые оценочные материалы

Оценочное средство 1.

Вид: Проверка лабораторных заданий по теме занятия.
Краткая характеристика: Задания построены с учетом изучаемой темы. Правильно выполненное задание позволяет оценить полученные ЗУН по теме, самостоятельную работу студента.

Оценочное средство 2.

Вид: Презентация результатов самостоятельной работы.
Краткая характеристика: Устная презентация предполагает умение обучающего работать с информацией, умение логично и четко формулировать свои мысли, владение культурой мышления, владение навыками презентации выполненной самостоятельной работы.

Оценочное средство 3.
Вид: Устный опрос
Краткая характеристика: Данное оценочное средство используется на каждом практическом занятии. Оцениваются фактические ЗУНы студентов, глубина понимания изучаемого материала, способности решить ситуационные задачи, а также навыки критической оценки информации, с которой обучающийся работал в процессе подготовки к занятию.

Оценочное средство 4.

Вид: Вопросы к промежуточной аттестации
Краткая характеристика: при проведении текущего контроля успеваемости и промежуточной аттестации применяется следующая система оценок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Промежуточная аттестация проходит в устной форме, по билетам.

Перечень примерных вопросов для проведения промежуточной аттестации в форме 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 зашиты 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 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. Криптогафическая стойкость.
27. Абсолютно стойкие криптосистемы.
28. Принципы Киркхоффса
29. Перспективные направления криптоанализа.

30. Основные принципы поточного шифрования.

Перечень примерных вопросов для проведения промежуточной аттестации в форме экзамена по модулю 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-неты. Принцип функционирования.
38. Бот-неты. 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 зашиты 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. Криптогафическая стойкость.
81. Абсолютно стойкие криптосистемы.
82. Принципы Киркхоффса
83. Перспективные направления криптоанализа,
84. квантовый криптоанализ.
85. Основные принципы поточного шифрования.

ФГАОУ ВО «Тюменский государственный университет»
Колледж искусственного интеллекта, креативного мышления и мастерства

УТВЕРЖДЕНО
Заместителем директора
ИИ Колледжа
Дубровиной Т.Л.
РАЗРАБОТЧИКИ
Дубровина Т.Л.
Волегова Е.А.

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
МДК.03.03 ОПРЕДЕЛЕНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ

для обучающихся по специальности: 10.02.05 Обеспечение информационной безопасности автоматизированных систем
форма обучения: очная
язык реализации: русский

Тюмень, 2026

1. Планируемые результаты освоения профессионального модуля

Код компетенции	Знания	Умения	Навыки
ПК 3.1; ПК 3.2; ПК 3.3; ПК 3.4; ПК 3.5.	З-1 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; З-2 номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; З-3 основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; З-4 основные способы физической защиты объектов информатизации; З-5 методики инструментального контроля эффективности защиты информации, обрабатываемой	У-1 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; У-2 применять технические средства для криптографической защиты информации конфиденциального характера; У-3 применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; У-4 применять инженерно-технические средства физической защиты объектов информатизации.	Н-1 Применения средств охранной сигнализации, охранного телевидения и систем контроля и управления доступом; Н-2 применения технических средств для криптографической защиты информации аппаратных средств; Н-3 применения технических средств для уничтожения информации и носителей информации.

	средствами вычислительной техники на объектах информатизации; З-6 номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.		

2. Структура и содержание профессионального модуля

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 (всего ак.ч.)	Курсовые работы (проекты)	Экзамен	Дифференцированный зачет
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
МДК.03.01 Техническая защита информации	5	144	–	121	19	–	4	–
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	5	141	–	111	6	20	4	–
МДК.03.03 Определение экономической эффективности деятельности организации.	5	36	–	31	3	–	–	2
Экзамен по модулю ПМ.03	5	4						
Итого по ПМ.03		***325***	**–**	***263***	***28***	***20***	***8***	***2***

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 подгруппам	Выполнение курсового проекта (работы)	Самостоятельная работа
МДК.03.01 Техническая защита информации.						
Раздел 1. Концепция инженерно-технической защиты информации.						
Содержание						
Тема 1.1. Предмет и задачи технической защиты информации. Общие положения защиты информации техническими средствами		2		6		1
Раздел 2. Теоретические основы инженерно-технической защиты информации.						
Содержание						
Тема 2.1. Информация как предмет защиты.		2		6		1
Тема 2.2. Технические каналы утечки информации.		2		6		1
Тема 2.3. Методы и средства технической разведки.		2		6		1
Раздел 3. Физические основы технической защиты информации.						
Содержание						
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.		2		6		1
Тема 3.2. Физические процессы при подавлении опасных сигналов.		2		6		1
Раздел 4. Системы защиты от утечки информации.						
Содержание						
Тема 4.1. Системы защиты от утечки информации по акустическому каналу.		2		6		1
Тема 4.2. Системы защиты от утечки информации по проводному каналу.		2		6		1
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу.		2		6		1
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу.		2		6		1
Тема 4.5. Системы защиты от утечки информации по телефонному каналу.		2		6		1

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу.		2		6		2
Тема 4.7. Системы защиты от утечки информации по оптическому каналу.		2		6		2
Раздел 5. Применение и эксплуатация технических средств защиты информации.						
Содержание						
Тема 5.1. Применение технических средств защиты информации.		2		6		2
Тема 5.2. Эксплуатация технических средств защиты информации.		2		6		2
Консультации	**1 ак.ч.**					
Промежуточная аттестация	**4 ак.ч. -** ***экзамен***					
Всего	***144***	***30***		***90***		***19***
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.						
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты.						
Содержание						
Тема 1.1. Цели и задачи физической защиты объектов информатизации. Общие сведения о комплексах инженерно-технических средств физической защиты		4		10		
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты.						
Содержание						
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты.		4		10		
Тема 2.2. Система контроля и управления доступом.		4		12		
Тема 2.3. Система телевизионного наблюдения.		4		12		
Тема 2.4. Система сбора, обработки, отображения и документирования информации.		4		12		
Тема 2.5 Система воздействия.		4		12		
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты.						
Содержание						
Тема 3.1 Применение инженерно-технических средств физической защиты. Эксплуатация инженерно-технических средств физической защиты.		6		12		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы.						6
Консультации	**1 ак.ч.**					
Промежуточная аттестация	**4 ак.ч. -** ***экзамен***					
Всего	***141***	***30***		***80***	***20***	***6***

МДК.03.03 Определение экономической эффективности деятельности организации.						
Раздел 1. Эффективность как бизнес-результат деятельности организации.						
Содержание						
Тема 1.1. Понятие и виды эффективности. Эффективность менеджмента, производства, финансовая эффективность, эффективность вложенного капитала, эффективность акционеров. Формирование стратегического подхода к управлению эффективностью бизнеса.		2		4		
Раздел 2. Методология сбалансированных систем показателей.						
Содержание						
Тема 2.1 Основные понятия стратегического менеджмента: целевое управление, миссия, видение, стратегические цели, критические факторы успеха. Движение информации о целях и степени их достижения. Мониторинг достижения целей. «Традиционные» организации и организации, ориентированные на стратегию.		2		4		
Раздел 3. Управление организацией с точки зрения управления по перспективам сбалансированных систем показателей.						
Содержание						
Тема 3.1 Управление организацией с точки зрения управления по перспективам сбалансированных систем показателей. Работа по формированию КПД по перспективам сбалансированных систем показателей.		2		4		
Раздел 4. Проектирование системы мотивации и мониторинга на основе ключевых показателей эффективности.						
Содержание						
Тема 4.1 Опережающие и результирующие KPI. Формирование дерева KPI. Методики рас KPI, Tableaudebord – система мониторинга и оценки эффективности управления бизнесом. Формирование комплекса показателей оценки деятельности компании.		2		4		
Тема 4.2 Операционная, тактическая, стратегическая панели индикаторов и их взаимосвязь с целевыми установками, определенными стратегией компании.		2		4		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы.						3

Консультации	**1 ак.ч.**					
Промежуточная аттестация	**2 ак.ч. – *дифференцированный зачет***					
Всего	**36**	**10**		**20**		**3**

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся осуществляются с применением оценочных материалов по профессиональному модулю (приложение № 1 - № 2 к рабочей программе профессионального модуля), включающих открытую (доступную к опубликованию) и закрытую (не размещаемую в свободном доступе) части.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

Учебно-методическое и информационное обеспечение реализации профессионального модуля сформировано с учетом требований ФГОС СПО и ПОП СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Для реализации основной образовательной программы подготовки квалифицированных рабочих, служащих по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем библиотечный фонд ИИ Колледжа имеет печатные и электронные образовательные и информационные ресурсы для использования в образовательном процессе.

4.1.1. Основная литература:

МДК.03.01 Техническая защита 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, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561717 (дата обращения: 22.04.2026).
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, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567283 (дата обращения: 22.04.2026).
3. 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: 22.04.2026).

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

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, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561717 (дата обращения: 22.04.2026).
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, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567283 (дата обращения: 22.04.2026).

3. 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: 22.04.2026).

МДК.03.03 Определение экономической эффективности деятельности организации

1. Шимко, П. Д. Экономика организации : учебник и практикум для среднего профессионального образования / П. Д. Шимко. — 5-е изд. — Москва : Издательство Юрайт, 2025. — 251 с. — (Профессиональное образование). — ISBN 978-5-534-18815-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561132 (дата обращения: 22.04.2026).

2. Основы экономической теории : учебник и практикум для среднего профессионального образования / под общей редакцией В. М. Пищулова. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 191 с. — (Профессиональное образование). — ISBN 978-5-534-16662-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562835 (дата обращения: 21.04.2026).

3. Борисов, Е. Ф. Основы экономики : учебник и практикум для среднего профессионального образования / Е. Ф. Борисов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 383 с. — (Профессиональное образование). — ISBN 978-5-534-02043-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560667 (дата обращения: 21.04.2026).

4.1.2. Дополнительная литература:

МДК.03.01 Техническая защита информации

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340 (дата обращения: 22.04.2026).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567521 (дата обращения: 22.04.2026).

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340 (дата обращения: 22.04.2026).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567521 (дата обращения: 22.04.2026).

МДК.03.03 Определение экономической эффективности деятельности организации

1. Дорман, В. Н. Экономика организации. Ресурсы коммерческой организации : учебное

пособие для среднего профессионального образования / В. Н. Дорман ; под научной редакцией Н. Р. Кельчевской. — Москва : Издательство Юрайт, 2024. — 121 с. — (Профессиональное образование). — ISBN 978-5-534-17063-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/532312 (дата обращения: 06.08.2026).

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:

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК 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.

Мультимедийная учебная аудитория для проведения практических занятий оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК 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 групповых и индивидуальных консультаций оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер (ПК). На ПК 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 оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК 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.

Аудитория для организации самостоятельной и воспитательной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры. На ПК 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.

Библиотека, читальный зал, коворкинг с выходом в интернет.

Приложение № 1
к рабочей программе
профессионального модуля

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
Защита информации техническими средствами
Открытая часть

1. Система оценивания

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

Промежуточная аттестация по МДК.03.01, МДК.03.02 в соответствии с учебным планом предусмотрена в форме экзамена, который проводится в традиционной форме по билетам.

Промежуточная аттестация по МДК.03.03 в соответствии с учебным планом предусмотрена в форме дифференцированного зачета, который проводится в традиционной форме по билетам.

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. Общие положения защиты информации техническими средствами	Лабораторная работа №1 Самостоятельная работа	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими	Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №1, самостоятельной работы 5 баллов
Тема 2.1. Информация как предмет защиты.	Лабораторная работа №2 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №2, самостоятельной работы 5 баллов

Тема 2.2. Технические каналы утечки информации.	Лабораторная работа №3 Самостоятельная работа	средствами обработки информации ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №3, самостоятельной работы 5 баллов
Тема 2.3. Методы и средства технической разведки.	Лабораторная работа №4 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №4, самостоятельной работы 5 баллов
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.	Лабораторная работа №5 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №5, самостоятельной работы 5 баллов
Тема 3.2. Физические процессы при подавлении опасных сигналов.	Лабораторная работа №6 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №6, самостоятельной работы 5 баллов

Тема 4.1. Системы защиты от утечки информации по акустическому каналу.	Лабораторная работа №7 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №7, самостоятельной работы 5 баллов
Тема 4.2. Системы защиты от утечки информации по проводному каналу.	Лабораторная работа №8 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №8, самостоятельной работы 5 баллов
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу.	Лабораторная работа №9 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №9, самостоятельной работы 5 баллов
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу.	Лабораторная работа №10 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №10, самостоятельной работы 5 баллов

Тема 4.5. Системы защиты от утечки информации по телефонному каналу.	Лабораторная работа №11 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №11, самостоятельной работы 5 баллов
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Лабораторная работа №12 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №12, самостоятельной работы 5 баллов
Тема 4.7. Системы защиты от утечки информации по оптическому каналу.	Лабораторная работа №13 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №13, самостоятельной работы 5 баллов
Тема 5.1. Применение технических средств защиты информации	Лабораторная работа №14 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №14, самостоятельной работы 5 баллов

Тема 5.2. Эксплуатация технических средств защиты информации.	Лабораторная работа №15 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №15, самостоятельной работы 5 баллов
Промежуточная аттестация обучающихся			
Экзамен, 5 семестр	Вопросы к экзамену – 30 вопросов	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	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

		ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	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.
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации			
Текущий контроль успеваемости			

Тема 1.1. Цели и задачи физической защиты объектов информатизации. Общие сведения о комплексах инженерно-технических средств физической защиты	Лабораторная работа №1	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №1 5 баллов
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты.	Лабораторная работа №2		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №2 5 баллов
Тема 2.2. Система контроля и управления доступом.	Лабораторная работа №3		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №3 5 баллов
Тема 2.3. Система телевизионного наблюдения.	Лабораторная работа №4		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №4 5 баллов

Тема 2.4. Система сбора, обработки, отображения и документирования информации.	Лабораторная работа №5		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №5 5 баллов
Тема 2.5 Система воздействия.	Лабораторная работа №6		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №6 5 баллов
Тема 3.1 Применение инженерно-технических средств физической защиты. Эксплуатация инженерно-технических средств физической защиты.	Лабораторная работа №7		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №7 5 баллов
Промежуточная аттестация обучающихся			
Экзамен, 5 семестр	Вопросы к экзамену – 30 вопросов	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	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

		ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	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.

МДК.03.03 Определение экономической эффективности деятельности организации.			
Текущий контроль успеваемости			
Тема 1.1. Понятие и виды эффективности. Эффективность менеджмента, производства, финансовая эффективность, эффективность вложенного капитала, эффективность акционеров. Формирование стратегического подхода к управлению эффективностью бизнеса. .	Лабораторная работа №1	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №1 5 баллов
Тема 2.1 Основные понятия стратегического менеджмента: целевое управление, миссия, видение, стратегические цели, критические факторы успеха. Движение информации о целях и степени их достижения. Мониторинг достижения целей. «Традиционные» организации и организации, ориентированные на стратегию	Лабораторная работа №2		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №2 5 баллов
Тема 3.1 Управление организацией с точки зрения управления по перспективам сбалансированных систем показателей. Работа по формированию КПД по перспективам сбалансированных систем показателей.	Лабораторная работа №3		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №3 5 баллов
Тема 4.1 Опережающие и результирующие KPI. Формирование дерева KPI. Методики рас KPI, Tableaudebord – система мониторинга и оценки эффективности управления бизнесом. Формирование комплекса показателей оценки	Лабораторная работа №4		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №4 5 баллов

деятельности компании			
Тема 4.2 Операционная, тактическая, стратегическая панели индикаторов и их взаимосвязь с целевыми установками, определенными стратегией компании	Лабораторная работа №5		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №5 5 баллов
Промежуточная аттестация обучающихся			
Дифференцированный зачет, 5 семестр	Вопросы к экзамену – 28 вопросов	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. ПК 3.5. Организовывать отдельные работы по	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.

		физической защите объектов информатизации.	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.

3. Типовые оценочные материалы

Оценочное средство 1.

Вид: Проверка лабораторных заданий по теме занятия.

Краткая характеристика: Задания построены с учетом изучаемой темы. Правильно выполненное задание позволяет оценить полученные ЗУН по теме, самостоятельную работу студента.

Оценочное средство 2.

Вид: Презентация результатов самостоятельной работы.

Краткая характеристика: Устная презентация предполагает умение обучающего работать с информацией, умение логично и четко формулировать свои мысли, владение культурой мышления, владение навыками презентации выполненной самостоятельной работы.

Оценочное средство 3.

Вид: Устный опрос

Краткая характеристика: Данное оценочное средство используется на каждом практическом занятии. Оцениваются фактические ЗУНы студентов, глубина понимания изучаемого материала, способности решить ситуационные задачи, а также навыки критической оценки информации, с которой обучающийся работал в процессе подготовки к занятию.

Оценочное средство 4.

Вид: Вопросы к промежуточной аттестации

Краткая характеристика: при проведении текущего контроля успеваемости и промежуточной аттестации применяется следующая система оценок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Промежуточная аттестация проходит в устной форме, по билетам.

Перечень примерных вопросов для проведения промежуточной аттестации в форме 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 примерных вопросов для проведения промежуточной аттестации в форме 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 примерных вопросов для проведения промежуточной аттестации в форме экзамена по МДК.03.03 Определение экономической эффективности деятельности организации.

1. Что такое корпоративное управление (corporate governance)?
2. В чем заключается проблема агентских отношений?
3. Каковы примеры конфликта интересов владельцев бизнеса и наемных менеджеров (директоров)?
4. Как происходило развитие корпоративного управления?
5. Каковы существующие кодексы корпоративного управления?
6. Как вопросы информационной прозрачности находят отражение в кодексах корпоративного управления?
7. Каковы современные системы корпоративной отчетности?
8. Какова роль Международных стандартов финансовой отчетности?
9. Какова роль отчетности в области устойчивого развития (GRI)?
10. Что такое стратегия и стратегический менеджмент?
11. Как корпоративное управление и стратегический менеджмент связаны междусобой?
12. Каковы три уровня стратегии?
13. В чем заключается сущность «рациональной модели» стратегического менеджмента?
14. Каковы основные стадии реализации «рациональной модели»?
15. Каковы функции обработки информации на каждой из стадий «рациональной модели»?
16. В чем заключаются достоинства и недостатки «рациональной модели»?
17. Что такое «продуманные» и «неотложные» стратегии?
18. Каковы альтернативные модели стратегического управления?
19. В чем заключается сущность «ограниченной рациональности»?
20. В чем заключается сущность инкрементализма?
21. В чем заключается сущность стратегического оппортунизма?
22. Каковы основные проблемы информационного обеспечения корпоративного управления и стратегического менеджмента?
23. В чем состоит сущность системы информационного обеспечения корпоративного управления и стратегического менеджмента?
24. Какова классификация информационных потоков системы информационного обеспечения корпоративного управления и стратегического менеджмента?
25. Каковы основные подсистемы (функциональные блоки) системы информационного обеспечения корпоративного управления и стратегического менеджмента?
26. Каковы основные характеристики блока стратегического анализа и моделирования?
27. Каковы основные характеристики блока управления по ключевым показателям?
28. Каковы основные характеристики блока корпоративного планирования и бюджетирования?

Перечень примерных вопросов для проведения промежуточной аттестации в форме экзамена по модулю 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: «оамносднрнзотнциаииооенрфибскиаопт». 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: «лбгтньефгжтвгцчесйоажгиттвияль». 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»
Колледж искусственного интеллекта, креативного мышления и мастерства

УТВЕРЖДЕНО
Заместителем директора
ИИ Колледжа
Дубровиной Т.Л.
РАЗРАБОТЧИКИ
Дубровина Т.Л.
Волегова Е.А.

ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН

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

МДК.04.01 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ВЫПОЛНЕНИЯ РАБОТ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН

для обучающихся по специальности: 10.02.05 Обеспечение информационной безопасности автоматизированных систем
форма обучения: очная
язык реализации: русский

Тюмень, 2026

1. Планируемые результаты освоения профессионального модуля

Код компетенции	Знания	Умения	Навыки
ДПКВ 1.1; ДПКВ 1.2; ДПКВ 1.3; ДПКВ 1.4; ДПКВ 1.5.	З-1 требования техники безопасности при работе с вычислительной техникой; З-2 основные принципы устройства и работы компьютерных систем и периферийных устройств; З-3 классификацию и назначение компьютерных сетей; З-4 виды носителей информации; З-5 программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета; З-6 основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.	У-1 выполнять требования техники безопасности при работе с вычислительно техникой; У-2 производить подключение блоков персонального компьютера и периферийны устройств; У-3 производить установку и замену расходных материалов для периферийны устройств и компьютерной оргтехники; У-4 диагностировать простейшие неисправности персонального компьютер периферийного оборудования и компьютерной оргтехники; У-5 выполнять инсталляцию системного и прикладного программного обеспечения; У-6 создавать и управлять содержимым документов с помощью текстовых процессоров; У-7 создавать и управлять содержимым электронных таблиц с помощью редактора таблиц; У-8 создавать и управлять содержимым презентаций с помощью редактора презентаций; У-9 использовать мультимедиа проектор для демонстрации презентаций;	Н-1 выполнения требований техники безопасности при работе с вычислительной техникой; Н-2 подключения блоков персонального компьютера и периферийны устройств; Н-3 установки и замены расходных материалов для периферийны устройств; Н-4 диагностики простейших неисправностей персонального компьютера.

		У-10 вводить, редактировать и удалять записи в базе данных; У-11 эффективно пользоваться запросами базы данных; У-12 создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; У-13 производить сканирование документов и их распознавание; У-14 производить распечатку, копирование и тиражирование документов на принтере и других устройствах; У-15 управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; У-16 осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; У-17 осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет-сайтов; У-18 осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; У-19 осуществлять резервное копирование и восстановление данных.	

2. Структура и содержание профессионального модуля

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 (всего ак.ч.)	Курсовые работы (проекты)	Экзамен
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
МДК.04.01 Теоретические основы выполнения работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин.	6	141	–	115	22	–	4
Экзамен по модулю ПМ.04	6	4					
Итого по ПМ.04:		***145***	**–**	***115***	***22***	**–**	***4***

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 подгруппам**	**Выполнение курсового проекта (работы)**	**Самостоятельная работа**
МДК.04.01 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН						
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения.						
Содержание						
Тема 1.1. Работа с устройствами компьютерной системы.		2				2

Тема 1.2. Работа с программным обеспечением компьютерной системы.		2				2
Тема 1.3. Диагностика неисправностей системы, ведение документации.		2				2
В том числе практические занятия:						
Тема 1.1. Работа с устройствами компьютерной системы.				8		
Тема 1.2. Работа с программным обеспечением компьютерной системы.				10		
Тема 1.3. Диагностика неисправностей системы, ведение документации.				8		
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах.						
Содержание						
Тема 2.1. Работа в текстовом процессоре.		2				2
Тема 2.2. Работа в редакторе электронных таблиц.		2				2
Тема 2.3. Работа в программе подготовки и просмотра презентаций.		2				2
Тема 2.4. Работа в системе управления базами данных.		2				2
Тема 2.5. Работа в графических редакторах.		2				2
В том числе практические занятия:						
Тема 2.1. Работа в текстовом процессоре.				10		
Тема 2.2. Работа в редакторе электронных таблиц.				8		
Тема 2.3. Работа в программе подготовки и просмотра презентаций.				10		
Тема 2.4. Работа в системе управления базами данных.				8		
Тема 2.5. Работа в графических редакторах.				10		
Раздел 3. Использование ресурсов технологий и сервисов Интернета.						
Содержание						
Тема 3.1. Работа с ресурсами Интернета.		4				3
В том числе практические занятия:						
Тема 3.1. Работа с ресурсами Интернета.				8		
Раздел 4. Обеспечение защиты информации в компьютерной системе.						
Содержание						
Тема 4.1. Защита информации при работе с офисными приложениями.		4				3
В том числе практические занятия:						
Тема 4.1. Защита информации при работе с офисными приложениями.				10		
Консультации	**1 ак.ч.**					
Промежуточная аттестация	**4 ак.ч. - *экзамен***					

Всего	**141**	**24**		**90**		**22**
Экзамен по модулю ПМ.04	**4 ак.ч.**					
Всего по модулю ПМ.04	**145**	**24**		**90**		**22**

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся осуществляются с применением оценочных материалов по профессиональному модулю (приложение № 1 - № 2 к рабочей программе профессионального модуля), включающих открытую (доступную к опубликованию) и закрытую (не размещаемую в свободном доступе) части.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

Учебно-методическое и информационное обеспечение реализации профессионального модуля сформировано с учетом требований ФГОС СПО и ПОП СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Для реализации основной образовательной программы подготовки квалифицированных рабочих, служащих по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем библиотечный фонд ИИ Колледжа имеет печатные и электронные образовательные и информационные ресурсы для использования в образовательном процессе.

4.1.1. Основная литература

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: 09.04.2026).

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: 09.04.2026).

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: 09.04.2026).

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: 09.04.2026). — Режим доступа: для авторизир. пользователей.

4.1.2. Дополнительная литература:

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: 09.04.2026).

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: 09.04.2026).

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 (дата обращения: 09.04.2026).

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 (дата обращения: 09.04.2026).

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:

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК 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.

Мультимедийная учебная аудитория для проведения практических занятий оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК 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 групповых и индивидуальных консультаций оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер (ПК). На ПК 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 оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК 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.

Аудитория для организации самостоятельной и воспитательной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры. На ПК 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.

Библиотека, читальный зал, коворкинг с выходом в интернет.

Приложение № 1
к рабочей программе
профессионального модуля

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин

Открытая часть

1. Система оценивания

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

Промежуточная аттестация в соответствии с учебным планом предусмотрена в форме экзамена, который проводится в традиционной форме по билетам.

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы *(виды и количество)*	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.04.01 Теоретические основы выполнения работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин			
Текущий контроль успеваемости			
Тема 1.1. Работа с устройствами компьютерной системы.	Лабораторная работа №1 Самостоятельная работа	ДПКВ 1.1 Проводить вычислительный процесс в соответствии рабочими программами; ДПКВ 1.2 Осуществлять подготовку технических носителей информации на устройствах подготовки данных и их контроль; ДПКВ 1.3 Проводить наблюдение за работой электронно-вычислительных машин; ДПКВ 1.4 Устанавливать причины сбоев работы электронно-вычислительных машинв процессе обработки информации;	Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №1 - 5 баллов
Тема 1.2. Работа с программным обеспечением компьютерной системы.	Лабораторная работа №2 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №2 - 5 баллов
Тема 1.3. Диагностика неисправностей системы, ведение документации.	Лабораторная работа №3 Самостоятельная работа	ДПКВ 1.5 Вести учет использования машинного времени в замеченных дефектах работы машины.	Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №3 5 баллов
Тема 2.1. Работа в текстовом процессоре.	Лабораторная работа №4 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях.

			Экспертная оценка выполнения лабораторной работы №4 5 баллов
Тема 2.2. Работа в редакторе электронных таблиц.	Лабораторная работа №5 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №5 5 баллов
Тема 2.3. Работа в программе подготовки и просмотра презентаций.	Лабораторная работа №6 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №6 5 баллов
Тема 2.4. Работа в системе управления базами данных.	Лабораторная работа №7 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №7 5 баллов
Тема 2.5. Работа в графических редакторах.	Лабораторная работа №8 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №8 5 баллов
Тема 3.1. Работа с ресурсами Интернета.	Лабораторная работа №9 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №9 5 баллов
Тема 4.1. Защита информации при работе с офисными приложениями.	Лабораторная работа №10 Самостоятельная работа		Экспертное наблюдение и оценивание ЗУН на теоретических и лабораторных занятиях. Экспертная оценка выполнения лабораторной работы №10

			5 баллов
Промежуточная аттестация обучающихся			
Экзамен, 6 семестр	Вопросы для экзамена – 55 вопросов	ДПКВ 1.1 Проводить вычислительный процесс в соответствии рабочими программами; ДПКВ 1.2 Осуществлять подготовку технических носителей информации на устройствах подготовки данных и их контроль; ДПКВ 1.3 Проводить наблюдение за работой электронно-вычислительных машин; ДПКВ 1.4 Устанавливать причины сбоев работы электронно-вычислительных машин в процессе обработки информации; ДПКВ 1.5 Вести учет использования машинного времени в замеченных дефектах работы машины.	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.

3. Типовые оценочные материалы

Оценочное средство 1.

Вид: Проверка лабораторных заданий по теме занятия.

Краткая характеристика: Задания построены с учетом изучаемой темы. Правильно выполненное задание позволяет оценить полученные ЗУН по теме, самостоятельную работу студента.

Оценочное средство 2.

Вид: Презентация результатов самостоятельной работы.

Краткая характеристика: Устная презентация предполагает умение обучающего работать с информацией, умение логично и четко формулировать свои мысли, владение культурой мышления, владение навыками презентации выполненной самостоятельной работы.

Оценочное средство 3.

Вид: Устный опрос

Краткая характеристика: Данное оценочное средство используется на каждом практическом занятии. Оцениваются фактические ЗУНы студентов, глубина понимания изучаемого материала, способности решить ситуационные задачи, а также навыки критической оценки информации, с которой обучающийся работал в процессе подготовки к занятию.

Оценочное средство 4.

Вид: Вопросы к экзамену

Краткая характеристика: при проведении текущего контроля успеваемости и промежуточной аттестации применяется следующая система оценок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Экзамен проходит в устной форме, по билетам.

Перечень примерных вопросов для проведения промежуточной аттестации в форме экзамена по МДК.04.01 Теоретические основы выполнения работ по профессии 16199 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.
31. Эргономика рабочего места.
32. Математические выражения. Графические области. Решение уравнений.
33. Общие сведения об электронно – вычислительных машинах.
34. Роль вычислительной техники в автоматизированных системах управления.
35. Введение в компьютерные сети. Каналы передачи данных.
36. Построить таблицу истинности для предложенной формулы.
37. Дайте определение технологического процесса обработки отраслевой информации.
38. Классификации компьютерных сетей.
39. Доказать правильность выражения логической функции через базовую логическую функцию.
40. Перечислите факторы, характеризующие технологического процесса обработки отраслевой информации.
41. Топологии локальных компьютерных сетей.
42. Наберите следующий текст, растянув его на страницу и соблюдая все форматы абзацев и символов: выравнивание (по ширине); левые (1,25 см) и правые отступы (1см); расстояния между абзацами (1,15); тип (TimesNR), размер (12) и начертание (курсив) шрифтов.
43. Дайте определение стандартизации технологического процесса обработки информации.
44. Принципы построения сети Интернет.
45. Создайте документ OpenPffice 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.).
46. Назовите этапы технологического процесса обработки отраслевой информации.
47. Глобальная компьютерная сеть.
48. Охарактеризуйте каждый этап технологического процесса обработки отраслевой информации.
49. Методы и средства защиты информации в компьютерных системах. Информационная безопасность и ее компоненты.
50. Понятие информации, информационных технологий. Классификация информационных технологий.
51. Методы и средства защиты в компьютерных системах.
52. Основные методы и средства обработки, хранения, передачи и накопления информации.
53. Системы счисления.
54. Основные приемы работы, элементы текстового редактора.
55. Наберите и отформатируйте текст по образцу, добавьте рамку на страницу.