Приложение
к ОПОП СПО 09.02.13 Интеграция решений с применением технологий искусственного интеллекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

Государственное бюджетное профессиональное образовательное учреждение Республики Дагестан «Технический колледж имени Р.Н. Ашуралиева»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по междисциплинарному курсу

междисциплинарного курса МДК.04.02 Обеспечение качества компьютерных систем

Специальность: 09.02.13 Интеграция решений с применением технологий искусственного интеллекта

Квалификация выпускника: специалист по работе с искусственным интеллектом

Махачкала 2025

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Фонд оценочных средств (далее – ФОС) дисциплины междисциплинарного курса МДК. 04.02. Обеспечение качества функционирования компьютерных систем является частью программы подготовки специалистов среднего звена специальности 09.02.13 Интеграция решений с применением технологий искусственного интеллекта.

ФОС позволяет оценить достижение, запланированных по междисциплинарному курсу, результатов обучения.

ФОС включают оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации по междисциплинарному курсу.

Текущий контроль успеваемости осуществляется с целью регулярного наблюдения за ходом поэтапного освоения обучающимися междисциплинарного курса, оптимизации управления образовательной деятельностью обучающихся, своевременной корректировки персональных образовательных результатов, обучающихся педагогическими средствами.

Текущему контролю успеваемости подлежат все обучающиеся, осваивающие междисциплинарный курс.

Текущий контроль проводится в пределах учебного времени, отведенного на изучение междисциплинарного курса традиционными и инновационными методами с использованием современных технологий.

Результаты текущего контроля успеваемости обучающихся в виде оценки в балльном выражении («5», «4», «3», «2») записываются в журнале учебных занятий.

Текущий контроль освоения обучающимися программного материала междисциплинарного курса может иметь следующие виды: оперативный и рубежный контроль.

Оперативный контроль проводится с целью объективной оценки качества освоения программы междисциплинарного курса, а также стимулирования учебной работы обучающихся, мониторинга результатов образовательной деятельности, подготовки к промежуточной аттестации и обеспечения максимальной эффективности учебно-воспитательного процесса.

Рубежный контроль является контрольной точкой и проводится с целью комплексной оценки уровня освоения программного материала.

Промежуточная аттестация по междисциплинарному курсу проводится с целью оценки уровня освоения теоретических знаний, умений, приобретенного практического опыта.

Формы и периодичность промежуточной аттестации по междисциплинарному курсу определяются учебным планом образовательной программы: экзамен 4 семестре.

Экзамен проводится непосредственно после завершения освоения междисциплинарного курса, в сроки, установленные календарным учебным графиком. Экзамен проводится в день, освобожденный от других форм учебной нагрузки.

Экзаменационные вопросы и задания составляются на основе рабочей программы междисциплинарного курса. Экзаменационные вопросы и задания должны соответствовать проверяемым результатам обучения и доводятся до сведения обучающихся в течение первых двух месяцев от начала обучения.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МЕЖДИСЦИПЛИНАРНОГО КУРСА

ПМ.04 Сопровождение и обслуживание программного обеспечения компьютерных систем направлен на формирование общих и профессиональных компетенций.

Освоение междисциплинарного курса должно способствовать формированию общих компетенций:

– ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

– ОК 02. Использовать современные средства поиска, анализа и интерпретации

информации, и информационные технологии для выполнения задач профессиональной деятельности.

- ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
- ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.
- ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
- ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
- ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
- ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
- ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

Освоение междисциплинарного курса должно способствовать формированию профессиональных компетенций:

- ПК 4.1. Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.
- ПК 4.2. Осуществлять измерения эксплуатационных характеристик программного обеспечения компьютерных систем
- ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами

В результате освоения междисциплинарного курса обучающийся должен получить практический опыт:

- выполнять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.
- настройка отдельных компонентов программного обеспечения компьютерных систем;
- измерять эксплуатационные характеристики программного обеспечения компьютерных систем на соответствие требованиям;
- обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

В результате освоения дисциплины обучающийся должен **уметь**:

Код умения	**Название умения**
У1	подбирать и настраивать конфигурацию программного обеспечения компьютерных систем
У2	проводить инсталляцию программного обеспечения компьютерных систем
У3	производить настройку отдельных компонент программного обеспечения компьютерных систем
У4	измерять и анализировать эксплуатационные характеристики качества программного обеспечения
У5	использовать методы защиты программного обеспечения компьютерных систем
У6	анализировать риски и характеристики качества программного обеспечения

У7	выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами

В результате освоения дисциплины обучающийся должен **знать:**

Код знания	**Название знания**
З1	основные методы и средства эффективного анализа функционирования программного обеспечения
З2	основные виды работ на этапе сопровождения программного обеспечения
З3	основные методы и средства эффективного анализа функционирования программного обеспечения
З4	основные принципы контроля конфигурации и поддержки целостности конфигурации ПО
З5	основные средства и методы защиты компьютерных систем программными и аппаратными средствами

Общие компетенции:

Код компетенции	**Формулировка компетенции**	**Знания, умения**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
		Знания: номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности

ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования
		Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
		Знания: психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе
		Знания: особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	**Умения:** описывать значимость своей специальности
		Знания: сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности
		Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и	**Умения:** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности

	поддержания необходимого уровня физической подготовленности.	**Знания:** роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

Профессиональные компетенции

Показатели освоения компетенции	Показатели освоения компетенции
ПК 4.1. Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.	**Практический опыт:** выполнять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем
	Умения: подбирать и настраивать конфигурацию программного обеспечения компьютерных систем
	Знания: основные методы и средства эффективного анализа функционирования программного обеспечения
ПК 4.2. Осуществлять измерения эксплуатационных характеристик программного обеспечения компьютерных систем.	**Практический опыт:** в выполнении отдельных видов работ на этапе поддержки программного обеспечения компьютерной системы
	Умения: производить настройку отдельных компонентов программного обеспечения компьютерных систем;
	Знания: основные виды работ на этапе сопровождения программного обеспечения; основные принципы контроля конфигурации и поддержки целостности конфигурации программного обеспечения
ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.	**Практический опыт:** в выполнении отдельных видов работ на этапе поддержки программного обеспечения компьютерной системы
	Умения: использовать методы защиты программного обеспечения компьютерных систем; проводить инсталляцию программного обеспечения компьютерных систем анализировать риски и характеристики качества программного обеспечения
	Знания: средства защиты программного обеспечения в компьютерных системах

3. ФОРМЫ И МЕТОДЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ

Формы текущего контроля по междисциплинарному курсу:

- устный опрос (фронтальный, индивидуальный, комбинированный);
- тестирование (письменное или компьютерное);

- письменная проверка (ответы на вопросы, решение задач и примеров, составление тезисов, рефератов, выполнение схем, выполнение заданий для самостоятельной работы и др.);
- практическая проверка (при проведении практических и лабораторных занятий, выполнении и защите курсовых проектов (работ));
- самоконтроль и взаимопроверка.

Возможны и другие формы текущего контроля успеваемости, в том числе инновационные на основе информационно-коммуникационных технологий.

Преподаватель на одном учебном занятии может использовать одну или несколько форм текущего контроля.

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 4.1 Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем.	Оценка **«отлично»** - предложенное программное обеспечение установлено, обоснован вариант конфигурации, обеспечен доступ различным категориям пользователей, обеспечена совместимость компонент с ранее установленными программными продуктами, проконтролировано качество функционирования с помощью встроенных средств. Оценка **«хорошо»** - предложенное программное обеспечение установлено, обоснован вариант конфигурации, обеспечен доступ различным категориям пользователей, обеспечена совместимость компонент с ранее установленными программными продуктами, проконтролировано качество функционирования. Оценка **«удовлетворительно»** - предложенное программное обеспечение установлено, обеспечен доступ различным категориям пользователей, обеспечена совместимость компонент с ранее установленными программными продуктами, проконтролировано качество функционирования	Экзамен в форме собеседования: практическое задание по инсталляции и настройке предложенного программного обеспечения (при необходимости используя руководство администратора). Защита отчетов по практическим и лабораторным работам
ПК 4.2 Осуществлять измерения эксплуатационных характеристик программного обеспечения компьютерных систем	Оценка **«отлично»** - определен полный набор качественных характеристик предложенного программного средства с помощью заданного набора метрик в том числе с использованием инструментальных средств; сделан вывод о соответствии заданным критериям; результаты сохранены в системе контроля версий. Оценка **«хорошо»** - определен набор качественных характеристик предложенного программного средства с помощью заданного набора метрик в том числе с использованием	Экзамен в форме собеседования: практическое задание по инсталляции и настройке предложенного программного обеспечения (при необходимости используя руководство администратора). Защита отчетов по практическим и лабораторным работам

	инструментальных средств; результаты сохранены в системе контроля версий. Оценка **«удовлетворительно»** - определены некоторые качественные характеристики предложенного программного средства из заданного набора метрик в том числе с использованием инструментальных средств; результаты сохранены в системе контроля версий.	
ПК 4.4 Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.	Оценка «отлично» - проанализированы риски и характеристики качества программного обеспечения; обоснованы и выбраны методы и средства защиты программного обеспечения; определен необходимый уровень защиты; защита программного обеспечения реализована на требуемом уровне. Оценка «хорошо» - проанализированы риски и характеристики качества программного обеспечения; выбраны методы и средства защиты программного обеспечения; защита программного обеспечения реализована на требуемом уровне. Оценка «удовлетворительно» - проанализированы риски и характеристики качества программного обеспечения; выбраны методы и средства защиты программного обеспечения; защита программного обеспечения реализована на стандартном	Экзамен в форме собеседования: практическое задание по инсталляции и настройке предложенного программного обеспечения (при необходимости используя руководство администратора). Защита отчетов по практическим и лабораторным работам

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	- Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач. - Адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	- Экспертное наблюдение за выполнением работ
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	- Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач. - Эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по	- Демонстрация ответственности за принятые решения. - Обоснованность самоанализа и коррекция результатов собственной работы	

финансовой грамотности в различных жизненных ситуациях		
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- Взаимодействовать с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик. - Обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	- Демонстрировать грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	- Соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- Эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик. - Демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	- Эффективность использовать средств физической культуры для сохранения и укрепления здоровья при выполнении профессиональной деятельности	
ОК 09. Использовать информационные технологии в профессиональной деятельности	- Эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	

4. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ МЕЖДИСЦИПЛИНАРНОГО КУРСА
МДК. 04.02. Обеспечение качества функционирования компьютерных систем

№	Наименование темы	Результаты обучения (освоенныеумения и знаний)	ПК, ОК, ЛР	Текущий контроль успеваемости	Промежуточная аттестация
1	2	3	4	5	6
	Раздел 2. Обеспечение качества компьютерных систем в процессе эксплуатации				
	МДК 04.02 Обеспечение качества функционирования компьютерных систем				
	Тема 4.2.1 Основные методы обеспечения качества функционирования	**З1 – З4, У1 – У4**	ОК 1 - ОК 9, ПК 4.1, ПК4.2	Устный опрос, тестирование, проверочные работы	Экзамен
1.	Понятие Жизненного цикла программного обеспечения. Этапы ЖЦ ПО	З1 – З4		Тестирование	
2.	Многоуровневая модель качества программного обеспечения			Тестирование (I, II)	
3.	Объекты уязвимости			Тестирование	
4.	Дестабилизирующие факторы и угрозы надежности			Проверочная работа	
5.	Методы предотвращения угроз надежности			Проверочная работа	
6.	Оперативные методы повышения надежности: временная, информационная, программная избыточность			Проверочная работа	
7.	Первичные ошибки, вторичные ошибки и их проявления			Устный опрос	
8.	Математические модели описания статистических характеристик ошибок в программах			Устный опрос	
9.	Анализ рисков и характеристик качества программного обеспечения при внедрении			Устный опрос	
10.	Целесообразность разработки модулей адаптации			Устный опрос	
11.	Тестирование программных продуктов	У1 – У4		Отчет по лабораторному занятию	
12.	Сравнение результатов тестирования с требованиями технического задания и/или спецификацией			Отчет по лабораторному занятию	
13.	Анализ рисков			Отчет по лабораторному занятию	
14.	Выявление первичных и вторичных ошибок			Отчет по лабораторному занятию	
15.	Разработка технического задания			Отчет по лабораторному занятию	
16.	Разработка руководства пользователя			Отчет по лабораторному занятию	
	Тема 4.2.2. Методы и средства защиты компьютерных систем	**З5, У5 – У7**	ОК 1 - ОК 9, ПК 4.4	Устный опрос, тестирование, проверочные работы	
17.	Вредоносные программы: классификация, методы обнаружения	З5		Проверочная работа	
18.	Антивирусные программы: классификация, сравнительный анализ			Тестирование	

19.	Несанкционированное использование информационных ресурсов. Нарушение информационного обслуживания			Тестирование	
20.	Файрвол: задачи, сравнительный анализ, настройка			Устный опрос	
21.	Информация об активных портах и соединениях. Поддержка невидимого режима			Устный опрос	
22.	Групповые политики. Аутентификация. Учетные записи			Тестирование	
23.	Тестирование защиты программного обеспечения			Устный опрос	
24.	Средства и протоколы шифрования сообщений			Тестирование	
25.	Протокол обмена сообщениями с использованием симметричного шифрования. Протокол обмена сообщениями с использованием шифрования с открытым ключом			Тестирование	
26.	Обнаружение вируса и устранение последствий его влияния	У5 - У7		Отчет по лабораторному занятию	
27.	Установка и настройка антивируса. Настройка обновлений с помощью зеркала			Отчет по лабораторному занятию	
28.	Настройка политики безопасности			Отчет по лабораторному занятию	
29.	Настройка браузера			Отчет по лабораторному занятию	
30.	Работа с реестром			Отчет по лабораторному занятию	
31.	Работа с программой восстановления файлов и очистки дисков			Отчет по лабораторному занятию	
32.	Измерения в сопровождении программного обеспечения			Отчет по лабораторному занятию	
33.	Поэтапное рассмотрение процесса сопровождения: подготовка, анализ проблем и изменений, внесение изменений			Отчет по лабораторному занятию	
34.	Работа по сопровождению программного обеспечения, реинжиниринг			Отчет по лабораторному занятию	
35.	Работы по модификации: формирование представления об эксплуатируемой/сопровождаемой системе			Отчет по лабораторному занятию	
	Самостоятельная работа обучающихся:				
	Набор средств моделирования объектно-ориентированных информационных систем Модели и стадии жизненного цикла. Эталонная модель процессов. Обеспечение процесса анализа и проектирования ИС возможностями CASE технологий. Процесс проектирования архитектуры системы Создание и разновидности автоматизированных систем управления. Сферы применения автоматизированных систем. Вид программного документа. Содержание программного документа. Надежность программного обеспечения информационных систем. Признаки появления ошибок.				

	Способы обеспечения и повышения надежности программ. Виды серверного программного обеспечения. Виды клиентского программного обеспечения.				

5. ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ
МДК 04.02. Обеспечение качества функционирования компьютерных систем

5.1. Типовые задания для оценки знаний и умений

ТЕМА 4.2.1. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ

Тест по теме 4.2.1.1. Понятие ЖЦ ПО. Этапы ЖЦ ПО

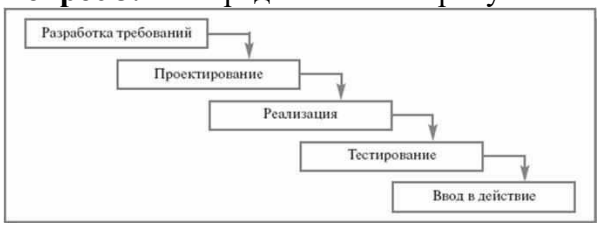
Вопрос 1. Жизненный цикл программы - это

a) это поиск способов повышения эффективности работы программы (быстрая работа, уменьшение затрат ресурсов ПК);
b) +это период времени, который начинается с момента принятия решения о необходимости создания программного продукта и заканчивается в момент его полного изъятия из эксплуатации
c) это экспериментальный анализ сложности алгоритма или экспериментальное сравнение нескольких алгоритмов, решающих одну и ту же задачу.

Вопрос 2. Программа - это

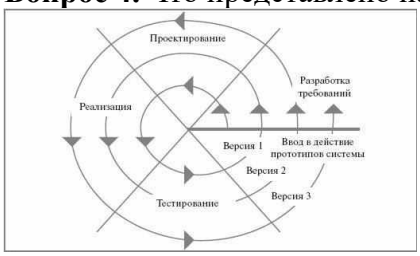
a) это точное описание порядка действий, которые должен выполнить исполнитель для решения задачи за конечное время.
b) это комплекс взаимосвязанных программ, предназначенный для поставки, передачи, продажи пользователю.
c) +это последовательность инструкций, предназначенная для исполнения вычислительной машиной

Вопрос 3. Что представлено на рисунке?



a) +это модель основной характеристикой которой является возможность перехода с одного этапа на следующий только после полного завершена работы на текущем этапе.
b) это поэтапная модель с промежуточным контролем.
c) это модель, в которой на каждом витке спирали выполняется создание очередной версии продукта, уточняются требования проекта, определяется его качество и планируются работы следующего витка.

Вопрос 4. Что представлено на рисунке?



a) это поэтапная модель с промежуточным контролем.
b) +это модель в которой на каждом витке спирали выполняется создание очередной версии продукта, уточняются требования проекта, определяется его качество и планируются работы следующего витка
c) это модель основной характеристикой которой является возможность перехода с одного этапа на следующий только после полного завершена работы на текущем этапе.

Вопрос 5. Поэтапная модель с промежуточным контролем
a) +Каскадная модель
b) Инкрементная модель
c) Спиральная модель

Вопрос 6. Формы записи алгоритма
Выберите несколько вариантов ответа
a) Алгоритмический
b) +Графический
c) Программный
d) +Словесный
e) Циклический

Вопрос 7. Расставьте по порядку этапы жизненного цикла программы
a) 1 анализ требований;
b) 2 определение спецификаций;
c) 3 проектирование;
d) 4 кодирование (программирование);
e) 5 тестирование и отладка;
f) 6 эксплуатация и сопровождение.

Вопрос 8. Тестирование программ - это
a) этап разработки компьютерной программы, в процессе которого проверяется работоспособность программы, не содержащей явных ошибок
b) этап разработки компьютерной программы, в процессе которого происходят обнаружение, локализация и устранение явных ошибок в программе
c) +проверка соответствия функциональности ПО решаемым задачам

Вопрос 9. Отладка программы
a) этап разработки компьютерной программы, в процессе которого проверяется работоспособность программы, не содержащей явных ошибок
b) +этап разработки компьютерной программы, в процессе которого происходят обнаружение, локализация и устранение явных ошибок в программе
c) это экспериментальный анализ сложности алгоритма или экспериментальное сравнение нескольких алгоритмов, решающих одну и ту же задачу.

Тест по теме 4.2.1.2. Многоуровневая модель качества (I)

Вопрос 1. Что такое программное обеспечение?
а) +совокупность программ, предназначенных для решение определенных задач на компьютере
б) закономерность систем, предназначенных для решение определенных задач на компьютере
в) совокупность программ, предназначенных для удаления задач на компьютере

2. Что такое доказательство правильности?
а) это системная или линейная методика, используемая для убеждения себя и других в том, что программа делает то, что должна делать
б) +это математическая или логическая методика, используемая для убеждения себя и других в том, что программа делает то, что должна делать
в) это программная система, используемая для убеждения себя и других в том, что программа делает то, что должна делать

3. Что определяет аспект, связанный с процессами ЖЦ ПО?
а) она достигается за счет использования процедур контроля программный продукт, качество внедрения ПО промежуточным продуктам на всех этапах их ЖЦ
б) процесс проверки качества, ориентированный на команду разработчиков
в) +степень формализации, достоверности самих процессов ЖЦ разработки ПО

4. Сколько характеристик входит в модель качества?
а) пять
б) +шесть
в) три

5. Функции бывают…?
а) +системные и определяющие
б) целевые и вспомогательные
в) прямые и косвенные

6. К подхарактеристикам надежности ПО относятся?
а) восстанавливаемость, безотказность, устойчивость к ошибкам
б) завершенность, отказоустойчивость, согласованность
в) +защищённость, функциональность, безотказность

7. Какой атрибут показывает способность ПО выполнять функции при аномальных условиях?
а) устойчивость к ошибкам
б) +надежность
в) восстанавливаемость

8. Что такое тестирование?
а) это совокупность программ, предназначенных для решения определенных задач на компьютере
б) +основной метод измерение качества, определение корректности и реальной надежности функционирование программ на каждом этапе разработки
в) описание функции в процессе решение задач

9. Какие оперативные методы используются для повышения надежности?
а) алгоритмическая, программная, системная
б) линейная, системная, временная
в) +временная, информационная, программная

10. Из чего состоит информационная избыточность?
а) является фактором, обеспечивающим безопасность функционирования систем.
б) +в дублировании накопленных и промежуточных данных, обрабатываемых программ
в) используется для контроля и обеспечение достоверности

12. Объектом уязвимости, влияющий на надежность ПС, является?
а) +ошибки программирования в текстах программ и описаниях данных, а также в исходной и результирующей документации на компоненты и ПС в целом;
б) информация, накопленная в базах данных, отражающая объекты внешней среды, и процессы ее обработки;
в) сбои и отказы в аппаратуре вычислительных средств;

13. Что из перечисленного не относится к методам предотвращения угроз надежности?
а) информационное предотвращение
б) систематическое тестирование
в) +предотвращение ошибок проектирования

Проверочная работа по теме 4.2.1.2. Многоуровневая модель качества (II)

Вопрос 1. Атрибут- это
1. измеримое физическое или абстрактное свойство продукта
2. измеримое физическое или виртуальное свойство продукта
3. + физическое или виртуальное свойство продукта, которое определяет потребитель

Вопрос 2. Метрика - это
1. текущий метод или шкала измерения
2. + определенный метод и шкала измерения
3. документ, определяющий параметры готового продукта

Вопрос 3. Измерение - это
1. + использование метрики для присвоения атрибуту продукта значения из шкалы.
2. использование метрики для присвоения атрибуту продукта значения перечня, утвержденного заказчиком
3. использование метрики для присвоения атрибуту продукта значения перечня, указанного в техническом задании

Вопрос 4. Модель качества - набор характеристик и связей между ними, ...
1. + обеспечивающий основу для определения требований к качеству и для оценки качества.
2. обеспечивающий параметры качества, заданные заказчиком
3. обеспечивающий параметры качества, заданные пользователем

Вопрос 5. Многоуровневая модель качества состоит из
1. атрибутов, целей и метрик качества
2. целей, задач, характеристик качества
3. + внешнего и внутреннего качества, а также внешней и внутренней меры качества

Вопрос 6. Многоуровневая модель качества включает в себя
1. + 6 факторов
2. 10 факторов
3. число факторов определяется в ТЗ

Вопрос 7. Какие из целей не относятся к многоуровневой модели качества?
Выберите несколько вариантов ответа

1. функциональность
2. надежность
3. + применимость
4. эффективность
5. сопровождаемость
6. мобильность
7. + независимость
8. + новизна

Вопрос 8. Мобильность- это
1. + способность программного обеспечения быть перенесенным из одного окружения в другое
2. способность программного обеспечения к адаптации
3. степень удобства внесения изменений

Вопрос 9. Сопровождаемость - это
1. + приспособленность программного средства к к модификации и изменению конфигурации и функций
2. приспособленность программного средства к модификации и изменению базового программного обеспечения
3. приспособленность программного средства к изменениям в техническом задании

Вопрос 10. Опорные метрики определяются путем
1. + непосредственных измерений или наблюдений
2. вычислений
3. с помощью процедур прогнозирования

Вопрос 11. Основные группы метрик-это
1. метрики процесса, метрики проекта, метрики продукта
2. метрики вычисления метрики прогнозирования, метрики наблюдения
3. + метрики внешние и метрики внутренние

Вопрос 12. Метрики использования служат для
1. + измерения степени удовлетворения потребностей пользователя при решении его задач
2. измерения степени использования функционала программного продукта при эксплуатации
3. измерения времени разработки программного продукта

Тест по теме 4.2.1.3. Объекты уязвимости

Вопрос 1. По отношению к защищаемой информации существуют следующие угрозы:
Выберите несколько вариантов ответа
1. Сокрытие
2. Несанкционированный доступ+
3. Утечка+
4. Разглашение+

Вопрос 2. Лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных

интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства это ...
Сформулируйте ответ - ... нарушитель

Вопрос 3. По источникам появления угрозы подразделяют на:
Выберите верный вариант ответа
1. Внешние и внутренние +
2. Естественные и искусственные
3. Пользовательские и сетевые

Вопрос 5. Можно выделить 3 основных мотива нарушений:
Выберите верные варианты ответов
1. Действие с целью мести
2. Корыстный интерес +
3. Безответственность +
4. Самоутверждение +

Проверочная работа по теме 4.2.1.4. Дестабилизирующие факторы и угрозы надежности

Вопрос 1. При облучении лазерным лучом стекол, зеркал, картин и других отражающих поверхностей создается - … канал утечки информации
Сформулируйте ответ
(оптико-электронный)

Вопрос 2. В зависимости от способов перехвата информации, от физической природы сигналов и среды их распространения технические каналы утечки информации можно разделить на:
Выберите верные варианты ответа
1. Параметрические+
2. Внешние
3. Дистанционные
4. Электромагнитные +
5. Электрические+

Вопрос 3. Сопоставьте каждому термину его определение:
1. Неопытный (невнимательный) пользователь
2. Мошенник
3. Внешний нарушитель (злоумышленник)
4. Любитель
5. Внутренний злоумышленник

а) Сотрудник организации, который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные аппаратные и программные средства от своего имени или от имени другого сотрудника.

б) Сотрудник организации, который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам организации с превышением своих полномочий, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства

в) Постороннее лицо или сотрудник организации, действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения безопасности информации, методов и средств взлома систем защиты, характерных для сетей общего пользования
г) Сотрудник организации, пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из спортивного интереса. Может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей других пользователей), недостатки в построении системы защиты и доступные ему штатные и нештатные программы
д) Сотрудник подразделения организации, зарегистрированный как пользователь системы, действующий целенаправленно из корыстны интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками организации
1-б, 2-д, 3-в, 4-г, 5-а

Проверочная работа по теме 4.2.1.5. Методы предотвращения угроз надежности (Методы тестирования)

Вопрос 1. Эти тесты считаются низкоуровневыми, близкими к исходному коду вашего приложения. Они нацелены на тестирование отдельных методов и функций внутри классов, тестирование компонентов и модулей, используемых вашей программой. Такие тесты в целом не требуют особых затрат на автоматизацию и могут отрабатывать крайне быстро, если задействовать сервер непрерывной интеграции (continuous integration server) - …
(Модульные тесты)

Вопрос 2. Такие тесты проверяют хорошо ли работают вместе сервисы и модули, используемые вашим приложением. Например, они могут тестировать интеграцию с базой данных или удостоверяться, что микросервисы правильно взаимодействуют друг с другом. Эти тесты запускаются с большими затратами, поскольку им необходимо, чтобы много частей приложения работало одновременно - …
(Интеграционные тесты)

Вопрос 3. Эти тесты основываются на требованиях бизнеса к приложению. Они лишь проверяют выходные данные после произведенного действия и не проверяют промежуточные состояния системы во время воспроизведения действия - …
(Функциональные тесты)

Вопрос 4. Такое тестирование имитирует поведение пользователя при взаимодействии с программным обеспечением. Этот тест проверяет насколько точно различные пользователи следуют предполагаемому сценарию работы приложения и могут быть достаточно простыми, допустим, выглядеть как загрузка веб-страницы или вход на сайт или в более сложном случае - подтверждение e-mail адреса, онлайн платежи и т.д.
(Сквозные тесты (End-to-end tests))

Вопрос 5. Эти тесты — это формальные тесты, которые проводятся, чтобы удостовериться, что система отвечает бизнес-запросам. Они требуют, чтобы приложение запускалось и работало, и имитируют действия пользователя. Такое тестирование может пойти дальше и измерить производительность системы и отклонить последние изменения, если конечные цели разработки не были достигнуты.
(Приемочные тесты)

Вопрос 6. Такие тесты проверяют поведение системы, когда она находится под существенной нагрузкой. Эти тесты нефункциональные и могут принимать разную форму, чтобы проверить надежность, стабильность и доступность платформы. Например, это может быть наблюдение за временем отклика при выполнении большого количества запросов или наблюдение за тем, как система ведет себя при взаимодействии с большими данными. Такие тесты по своей природе проводить достаточно затратно, но они могут помочь вам понять, какие внешние факторы могут уронить вашу систему.
(Тесты производительности)

Вопрос 7. Такие тесты — это базовые тесты, которые проверяют базовый функционал приложения. Они отрабатывают достаточно быстро и их цель дать понять, что основные функции системы работают как надо и не более того. Такое тестирование направлено на выявление явных ошибок. Эти тесты могут оказаться полезными сразу после сборки нового билда для проверки на то, можете ли вы запустить более дорогостоящие тесты, или сразу после развёртывания, чтобы убедиться, что приложение работает нормально в новой среде.
(Дымовое тестирование (Smoke testing))

Проверочная работа по теме 4.2.1.6. Оперативные методы повышения надежности: временная, информационная, программная избыточность

Вопрос 1. … использует часть производительности компьютера для контроля исполнения программ и восстановления вычислительного процесса. Как следствие при проектировании ПО необходимо предусматривать резерв производительности, обычно резерв составляет 5-10%.
(Временная избыточность)

Вопрос 2. … применяет в комплексах ПО несколько вариантов программ, различающихся алгоритмами решения задачи или программной реализации одного и того же алгоритма - ….
(Программная избыточность)

Вопрос 3. … заключается в резервировании (дублировании) исходных и промежуточных данных, что обеспечивает как обнаружение искажения данных, так и устранение ошибок.
(Информационная избыточность)

Вопрос 4. ... - позволяет облегчить проектирование и повысить надежность сложных программных комплексов. Структурное программирование развилось на основе технологии процедурного и модульного программирования, а также блочно-иерархического подхода; представляет собой технологию программирования, построенную на совокупности определенных принципов и правил, среди которых прежде всего можно выделить модульность структуры, иерархию модулей, нисходящее проектирование. - …
(*Структурное программирование)*

Вопрос 5. ... - позволяет уменьшить сложность комплекса программ и снизить вероятность появления ошибок из-за их неправильного использования. Совокупность данных можно разделить на два иерархических уровня: простые переменные и массивы. Простые переменные представляют собой минимальный компонент данных, имеющий имя и описание. Массивы образуются из нескольких простых переменных по определенным правилам объединения и имеют собственное имя, описание и структуру - …
(*Структурирование данных)*

Лабораторные занятия № 1 - 6:

1. Тестирование программных продуктов
2. Сравнение результатов тестирования с требованиями технического задания и/или спецификацией
3. Анализ рисков
4. Выявление первичных и вторичных ошибок
5. Разработка технического задания
6. Разработка руководства пользователя

ТЕМА 4.2.2. Методы и средства защиты компьютерных систем

Проверочная работа по теме 4.2.2.17. Вредоносные программы: классификация, методы обнаружения

Вопрос 1. Сопоставьте номер изображения и название программы

1)  3

2)  5

3)  1

4)  2

5)  6

6)  4

1) Antivir; 2) DrWeb; 3) Nod 32; 4) Antivirus Kaspersky; 5) Avast; 6) Antivirus Panda.

Вопрос 2. Определите истинность или ложность высказывания (да или нет):
1) -Почтовый червь активируется в тот момент, когда к вам поступает электронная почта
2) -Если компьютер не подключен к сети Интернет, в него не проникнут вирусы
3) -Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls
4) +Чтобы защитить компьютер недостаточно только установить антивирусную программу
5) +На Web-страницах могут находиться сетевые черви.

Вопрос 3. Вредоносные программы - это ….
1) шпионские программы
2) +программы, наносящие вред данным и программам, находящимся на компьютере
3) антивирусные программы
4) программы, наносящие вред пользователю, работающему на зараженном компьютере
5) троянские утилиты и сетевые черви

Вопрос 4. К вредоносным программам относятся
Выберите несколько вариантов ответа
1) +Потенциально опасные программы
2) +Вирусы, черви, трояны
3) +Шпионские и рекламные программы
4) Вирусы, программы-шутки, антивирусное программное обеспечение
5) Межсетевой экран, брандмауэр

Вопрос 5. Сетевые черви - это…
1) Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты
2) Вирусы, которые проникнув на компьютер, блокируют работу сети
3) Вирусы, которые внедряются в документы под видом макросов
4) Хакерские утилиты, управляющие удаленным доступом компьютера
5) +Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

Вопрос 6. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется
1) Загрузочный вирус; 2) Макровирус; 3) Троян; 4) Сетевой червь; 5) +Файловый вирус.

Вопрос 7. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию
Запишите ответ: _____
(Троян)

Вопрос 8. Компьютерные вирусы – это
Выберите несколько вариантов ответа
1) +Вредоносные программы, наносящие вред данным
2) Программы, уничтожающие данные на жестком диске
3) +Программы, которые могут размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы
4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера
5) Это скрипты, помещенные на зараженных интернет-страничках

Вопрос 9. Вирус внедряется в исполняемые файлы и при их запуске активируется
1) Загрузочный вирус; 2) Макровирус; 3) +Файловый вирус; 4) Сетевой червь; 5) Троян.

Вопрос 10. Укажите порядок действий при наличии признаков заражения компьютера
1) Сохранить результаты работы на внешнем носителе
2) Запустить антивирусную программу
3) Отключиться от глобальной или локальной сети
(3, 1, 2)

Вопрос 11. Вирус, поражающий документы, называется
1) Троян; 2) Файловый вирус; 3) +Макровирус; 4) Загрузочный вирус; 5) Сетевой червь.

Тест по теме 4.2.2.18. Антивирусные программы: классификация, сравнительный анализ

Вопрос 1. Что такое компьютерный вирус?
1) Прикладная программа
2) Системная программа
3) +Программа, выполняющая на компьютере несанкционированные действия
4) База данных

Вопрос 2. Основные типы компьютерных вирусов
1) Аппаратные, программные, загрузочные
2) +Программные, загрузочные, макровирусы
3) Файловые, программные, макровирусы

Вопрос 3. Этапы действия программного вируса
1) +Размножение, вирусная атака
2) Запись в файл, размножение
3) Запись в файл, размножение, уничтожение программы

Вопрос 4. В чем заключается размножение программного вируса?
1) Программа-вирус один раз копируется в теле другой программы
2) +Вирусный код неоднократно копируется в теле другой программы

Вопрос 5. Что такое вирусная атака?
1) Неоднократное копирование кода вируса в код программы
2) Отключение компьютера в результате попадания вируса
3) +Нарушение работы программы, уничтожение данных, форматирование жесткого диска

Вопрос 6. Какие существуют методы реализации антивирусной защиты?
1) +Аппаратные и программные
2) Программные и административные
3) Только программные

Вопрос 7. Какие существуют основные средства защиты данных?
1) +Резервное копирование наиболее ценных данных
2) Аппаратные средства
3) Программные средства

Вопрос 8. Какие существуют вспомогательные средства защиты?
1) Аппаратные средства
2) Программные средства
3) +Аппаратные средства и антивирусные программы
4) Административные методы и антивирусные программы

Вопрос 9. На чем основано действие антивирусной программы?

1) На ожидании начала вирусной атаки.
2) +На сравнении программных кодов с известными вирусами.
3) На удалении зараженных файлов.

Вопрос 10. Какие программы относятся к антивирусным
1) +AVP, DrWeb, Norton AntiVirus.
2) MS-DOS, MS Word, AVP.
3) MS Word, MS Excel, Norton Commander.

Тест по теме 4.2.2.19. Несанкционированное использование информационных ресурсов. Нарушение информационного обслуживания

Вопрос 1. К правовым методам, обеспечивающим информационную безопасность, относятся:
1) Разработка аппаратных средств обеспечения правовых данных
2) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3) +Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Вопрос 2. Основными источниками угроз информационной безопасности являются все указанное в списке:
1) Хищение жестких дисков, подключение к сети, инсайдерство
2) +Перехват данных, хищение данных, изменение архитектуры системы
3) Хищение данных, подкуп системных администраторов, нарушение регламента работы

Вопрос 3. Виды информационной безопасности
1) +Персональная, корпоративная, государственная
2) Клиентская, серверная, сетевая
3) Локальная, глобальная, смешанная

Вопрос 4. Цели информационной безопасности – своевременное обнаружение, предупреждение
1) +Несанкционированного доступа, воздействия в сети
2) Инсайдерства в организации
3) Чрезвычайных ситуаций

Вопрос 5. Основные объекты информационной безопасности
1) +Компьютерные сети, базы данных
2) Информационные системы, психологическое состояние пользователей
3) Бизнес-ориентированные, коммерческие системы

Вопрос 6. Основными рисками информационной безопасности являются
1) Искажение, уменьшение объема, перекодировка информации
2) Техническое вмешательство, выведение из строя оборудования сети
3) +Потеря, искажение, утечка информации

Вопрос 7. К основным принципам обеспечения информационной безопасности относится
1) +Экономической эффективности системы безопасности
2) Многоплатформенной реализации системы
3) Усиления защищенности всех звеньев системы

Вопрос 8. Основными субъектами информационной безопасности являются
1) Руководители, менеджеры, администраторы компаний

2) +Органы права, государства, бизнеса
3) Сетевые базы данных, файрволы

Вопрос 8. К основным функциям системы безопасности можно отнести все перечисленное
1) +Установление регламента, аудит системы, выявление рисков
2) Установка новых офисных приложений, смена хостинг-компании
3) Внедрение аутентификации, проверки контактных данных пользователей

Вопрос 10. Принципом информационной безопасности является принцип недопущения
1) +Неоправданных ограничений при работе в сети (системе)
2) Рисков безопасности сети, системы
3) Презумпции секретности

Вопрос 11. Принципом политики информационной безопасности является принцип
1) +Невозможности миновать защитные средства сети (системы)
2) Усиления основного звена сети, системы
3) Полного блокирования доступа при риск-ситуациях

Вопрос 12. Принципом политики информационной безопасности является принцип
1) +Усиления защищенности самого незащищенного звена сети (системы)
2) Перехода в безопасное состояние работы сети, системы
3) Полного доступа пользователей ко всем ресурсам сети, системы

Вопрос 13. Принципом политики информационной безопасности является принцип
1) +Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
2) Одноуровневой защиты сети, системы
3) Совместимых, однотипных программно-технических средств сети, системы

Вопрос 14. К основным типам средств воздействия на компьютерную сеть относится
1) Компьютерный сбой
2) +Логические закладки («мины»)
3) Аварийное отключение питания

Вопрос 15. Когда получен спам по e-mail с приложенным файлом, следует
1) Прочитать приложение, если оно не содержит ничего ценного – удалить
2) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
3) +Удалить письмо с приложением, не раскрывая (не читая) его

Вопрос 16. Принцип Кирхгофа
1) Секретность ключа определена секретностью открытого сообщения
2) Секретность информации определена скоростью передачи данных
3) +Секретность закрытого сообщения определяется секретностью ключа

Вопрос 17. ЭЦП – это
1) Электронно-цифровой преобразователь
2) +Электронно-цифровая подпись
3) Электронно-цифровой процессор

Вопрос 18. Наиболее распространены угрозы информационной безопасности корпоративной системы
1) Покупка нелицензионного ПО
2) +Ошибки эксплуатации и неумышленного изменения режима работы системы

3) Сознательного внедрения сетевых вирусов

Вопрос 19. Наиболее распространены угрозы информационной безопасности сети
1) Распределенный доступ клиент, отказ оборудования
2)Моральный износ сети, инсайдерство
3) +Сбой (отказ) оборудования, нелегальное копирование данных

Вопрос 20. Наиболее распространены средства воздействия на сеть офиса
1) Слабый трафик, информационный обман, вирусы в интернет
2) +Вирусы в сети, логические мины (закладки), информационный перехват
3) Компьютерные сбои, изменение администрирования, топологии

Вопрос 21. Утечкой информации в системе называется ситуация, характеризуемая
1) +Потерей данных в системе
2) Изменением формы информации
3) Изменением содержания информации

Вопрос 22. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются
1) +Целостность
2) Доступность
3) Актуальность

Вопрос 23. Угроза информационной системе (компьютерной сети) – это
1) +Вероятное событие
2) Детерминированное (всегда определенное) событие
3) Событие, происходящее периодически

Вопрос 24. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется
1) Регламентированной
2) Правовой
3) +Защищаемой

Вопрос 25. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке
1) +Программные, технические, организационные, технологические
2) Серверные, клиентские, спутниковые, наземные
3) Личные, корпоративные, социальные, национальные

Вопрос 26. Окончательно, ответственность за защищенность данных в компьютерной сети несет
1) +Владелец сети
2) Администратор сети
3) Пользователь сети

Вопрос 27. Политика безопасности в системе (сети) – это комплекс
1) +Руководств, требований обеспечения необходимого уровня безопасности
2) Инструкций, алгоритмов поведения пользователя в сети
3) Нормы информационного права, соблюдаемые в сети

Вопрос 28. Наиболее важным при реализации защитных мер политики безопасности является:
1) Аудит, анализ затрат на проведение защитных мер
2) Аудит, анализ безопасности
3) +Аудит, анализ уязвимостей, риск-ситуаций

Тест по теме 4.2.2.22. Групповые политики. Аутентификация. Учетные записи

Вопрос 1. Какого уровня информационной безопасности при аутентификации не существует
а) статическая аутентификация
б) временная аутентификация
в) устойчивая аутентификация
г) постоянная аутентификация

Вопрос 2. Какую из функций обеспечивает идентификация
а) вход в безопасный режим
б) допуск в систему
в) отключение всех функций системы

Вопрос 3. Наиболее распространенный метод аутентификации
а) биометрическая аутентификация
б) аутентификация посредством GPS
в) аутентификация по паролям
г) многофакторная аутентификация

Вопрос 4. Какого элемента не существует в системе аутентификации
а) субъект
б) характеристика субъекта
в) объект
г) механизм аутентификации

Вопрос 5. Какого значения параметра не предусмотрено в *Политике паролей*
а) минимальная длина пароля
б) разнообразные подсказки при вводе пароля
в) максимальный срок действия пароля
г) хранение паролей, использующее необратимое шифрование

Вопрос 6. Какой из параметров используется при блокировке учетной записи
а) продолжительность блокировки учетной записи
б) действия, выполняемые при блокировке учетной записи
в) сообщения в центр поддержки при блокировке учетной записи

Проверочная работа по теме 4.2.2.24. Средства и протоколы шифрования сообщений

Вопрос 1. Что такое шифрование?
а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого+
б) совокупность тем или иным способом структурированных данных и комплексом

аппаратно-программных средств
в) удобная среда для вычисления конечного пользователя

Вопрос 2. Что такое кодирование?
а) преобразование обычного, понятного текста в код+
б) преобразование
в) написание программы
Вопрос 3. Для восстановления защитного текста требуется:
а) ключ+
б) матрица
в) вектор

Вопрос 4. Сколько лет назад появилось шифрование?
а) четыре тысячи лет назад+
б) две тысячи лет назад
в) пять тысяч лет назад

Вопрос 5. Первое известное применение шифра:
а) египетский текст+
б) русский
в) нет правильного ответа

Вопрос 6. Секретная информация, которая хранится в Windows:
а) пароли для доступа к сетевым ресурсам+
б) пароли для доступа в Интернет+
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере+

Вопрос 7. Что такое алфавит?
а) конечное множество используемых для кодирования информации знаков+
б) буквы текста
в) нет правильного ответа

Вопрос 8. Что такое текст?
а) упорядоченный набор из элементов алфавита+
б) конечное множество используемых для кодирования информации знаков
в) все правильные

Вопрос 9. Выберите примеры алфавитов
а) Z256 – символы, входящие в стандартные коды ASCII и КОИ-8+
б) восьмеричный и шестнадцатеричный алфавиты+
в) AEE

Вопрос 10. Что такое шифрование?
а) преобразовательный процесс исходного текста в зашифрованный+
б) упорядоченный набор из элементов алфавита
в) нет правильного ответа

Вопрос 11. Что такое дешифрование?
а) на основе ключа шифрованный текст преобразуется в исходный+
б) пароли для доступа к сетевым ресурсам

в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

Вопрос 12. Что представляет собой криптографическая система?
а) семейство T преобразований открытого текста, члены его семейства индексируются символом k+
б) программу
в) систему
Вопрос 13. Что такое пространство ключей k?
а) набор возможных значений ключа+
б) длина ключа
в) нет правильного ответа

Вопрос 14. На какие виды подразделяют криптосистемы?
а) симметричные+
б) ассиметричные+
в) с открытым ключом+

Вопрос 15. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:
а) 1+
б) 2
в) 3

Вопрос 16. Количество используемых ключей в системах с открытым ключом:
а) 2+
б) 3
в) 1

Вопрос 17. Ключи, используемые в системах с открытым ключом:
а) открытый+
б) закрытый+
в) нет правильного ответа

Вопрос 18. Выберите то, как связаны ключи друг с другом в системе с открытым ключом:
а) математически+
б) логически
в) алгоритмически

Вопрос 19. Что принято называть электронной подписью?
а) присоединяемое к тексту его криптографическое преобразование+
б) текст
в) зашифрованный текст

Вопрос 20. Что такое криптостойкость?
а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа+
б) свойство гаммы
в) все ответы верны

Вопрос 21. Выберите то, что относится к показателям криптостойкости:
а) количество всех возможных ключей+

б) среднее время, необходимое для криптоанализа+
в) количество символов в ключе

Вопрос 22. Требования, предъявляемые к современным криптографическим системам защиты информации:
а) знание алгоритма шифрования не должно влиять на надежность защиты+
б) структурные элементы алгоритма шифрования должны быть неизменными+
в) не должно быть простых и легко устанавливаемых зависимостью между ключами +последовательно используемыми в процессе шифрования+

Вопрос 23. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
а) длина шифрованного текста должна быть равной лине исходного текста+
б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа+
в) нет правильного ответа

Вопрос 24. Основными современными методами шифрования являются:
а) алгоритм гаммирования+
б) алгоритмы сложных математических преобразований+
в) алгоритм перестановки+

Вопрос 25. Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности?
а) алгоритмом гаммирования+
б) алгоритмом перестановки
в) алгоритмом аналитических преобразований

Вопрос 26. Чем являются символы оригинального текста, меняющиеся местами по определенному принципу, которые являются секретным ключом?
а) алгоритм перестановки+
б) алгоритм подстановки
в) алгоритм гаммирования

Вопрос 27. Самая простая разновидность подстановки:
а) простая замена+
б) перестановка
в) простая перестановка

Вопрос 28. Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера:
а) 3+
б) 4
в) 5

Вопрос 29. Таблицы Вижинера, применяемые для повышения стойкости шифрования:
а) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке+
б) в качестве ключа используется случайность последовательных чисел+
в) нет правильного ответа

Вопрос 30. Суть метода перестановки:
а) символы шифруемого текста переставляются по определенным правилам внутри

шифруемого блока символов+
б) замена алфавита
в) все правильные

Проверочная работа по теме 4.2.2.25. Протокол обмена сообщениями с использованием симметричного шифрования. Протокол обмена сообщениями с использованием шифрования с открытым ключом

Вопрос 1. Цель криптоанализа
а) Определение стойкости алгоритма+
б) Увеличение количества функций замещения в криптографическом алгоритме
в) Уменьшение количества функций подстановок в криптографическом алгоритме
г) Определение использованных перестановок

Вопрос 2. По какой причине произойдет рост частоты применения брутфорс-атак?
а) Возросло используемое в алгоритмах количество перестановок и замещений
б) Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
в) Мощность и скорость работы процессоров возросла+
г) Длина ключа со временем уменьшилась

Вопрос 3. Не будет являться свойством или характеристикой односторонней функции хэширования
а) Она преобразует сообщение произвольной длины в значение фиксированной длины
б) Имея значение дайджеста сообщения, невозможно получить само сообщение
в) Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
г) Она преобразует сообщение фиксированной длины в значение переменной длины+

Вопрос 4. Выберите то, что указывает на изменение сообщения
а) Изменился открытый ключ
б) Изменился закрытый ключ
в) Изменился дайджест сообщения+
г) Сообщение было правильно зашифровано

Вопрос 5. Алгоритм американского правительства, который предназначен для создания безопасных дайджестов сообщений
а) Data Encryption Algorithm
б) Digital Signature Standard
в) Secure Hash Algorithm+
г) Data Signature Algorithm

Вопрос 6. Выберите то, что лучшеописывает отличия между HMAC и CBC-MAC?
а) HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности
б) HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы
в) HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC+

г) HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком

Вопрос 7. Определите преимущество RSA над DSA?
а) Он может обеспечить функциональность цифровой подписи и шифрования+
б) Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
в) Это блочный шифр и он лучше поточного
г) Он использует одноразовые шифровальные блокноты

Вопрос 8. С какой целью многими странами происходит ограничение использования и экспорта криптографических систем?
а) Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
б) Эти системы могут использоваться некоторыми странами против их местного населения
в) Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования+
г) Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему

Вопрос 9. Выберите то, что используют для создания цифровой подписи:
а) Закрытый ключ получателя
б) Открытый ключ отправителя
в) Закрытый ключ отправителя+
г) Открытый ключ получателя

Вопрос 10. Выберите то, что лучше всего описывает цифровую подпись:
а) Это метод переноса собственноручной подписи на электронный документ
б) Это метод шифрования конфиденциальной информации
в) Это метод, обеспечивающий электронную подпись и шифрование
г) Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения+

Вопрос 11. Эффективная длина ключа в DES:
а) 56+
б) 64
в) 32
г) 16

Вопрос 12. Причина, по которой удостоверяющий центр отзывает сертификат:
а) Если открытый ключ пользователя скомпрометирован
б) Если пользователь переходит на использование модели PEM, которая использует сеть доверия
в) Если закрытый ключ пользователя скомпрометирован+
г) Если пользователь переходит работать в другой офис

Вопрос 13. Выберите то, что лучше всего описывает удостоверяющий центр?
а) Организация, которая выпускает закрытые ключи и соответствующие алгоритмы
б) Организация, которая проверяет процессы шифрования
в) Организация, которая проверяет ключи шифрования
г) Организация, которая выпускает сертификаты+

Вопрос 14. Расшифруйте аббревиатуру DEA
а) Data Encoding Algorithm
б) Data Encoding Application
в) Data Encryption Algorithm+
г) Digital Encryption Algorithm

Вопрос 15. Разработчик первого алгоритма с открытыми ключами
а) Ади Шамир
б) Росс Андерсон
в) Брюс Шнайер
г) Мартин Хеллман+

Вопрос 16. Процесс, выполняемый после создания сеансового ключа DES
а) Подписание ключа
б) Передача ключа на хранение третьей стороне (key escrow)
в) Кластеризация ключа
г) Обмен ключом+

Вопрос 17. Количество циклов перестановки и замещения, выполняемый DES
а) 16+
б) 32
в) 64
г) 56

Вопрос 18. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты
а) Оно обеспечивает проверку целостности и правильности данных
б) Оно требует внимательного отношения к процессу управления ключами+
в) Оно не требует большого количества системных ресурсов
г) Оно требует передачи ключа на хранение третьей стороне (escrowed)

Вопрос 19. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст
а) Коллизия
б) Хэширование
в) MAC
г) Кластеризация ключей+

Вопрос 20. Определение фактора трудозатрат для алгоритма
а) Время зашифрования и расшифрования открытого текста
б) Время, которое займет взлом шифрования+
в) Время, которое занимает выполнение 16 циклов преобразований
г) Время, которое занимает выполнение функций подстановки

Вопрос 21. Основная цельиспользования одностороннего хэширования пароля пользователя
а) Это снижает требуемый объем дискового пространства для хранения пароля пользователя
б) Это предотвращает ознакомление кого-либо с открытым текстом пароля+

в) Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом
г) Это предотвращает атаки повтора (replay attack)

Вопрос 22. Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя
а) ECC
б) RSA+
в)DES
г) Диффи-Хеллман

Вопрос 23. Что является описанием разницы алгоритмов DES и RSA
а) DES – это симметричный алгоритм, а RSA – асимметричный +
б) DES – это асимметричный алгоритм, а RSA – симметричный
в) Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша
г) DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений

Вопрос 24. Алгоритм, использующий симметричный ключ и алгоритм хэширования
а) HMAC+
б) 3DES
в) ISAKMP-OAKLEY
г) RSA

Вопрос 25. Количество способов гаммирования
а) 2+
б) 5
в) 3

Вопрос 26. Показатель стойкости шифрования методом гаммирования
а) свойство гаммы+
б) длина ключа
в) нет правильного ответа

Вопрос 27. То, что применяют в качестве гаммы
а) любая последовательность случайных символов+
б) число
в) все ответы верны

Вопрос 28. Метод, который применяют при шифровании с помощью аналитических преобразований
а) алгебры матриц+
б) матрица
в) факториал

Вопрос 29. То, что применяют в качестве ключа при шифровании с помощью аналитических преобразований
а) матрица А+
б) вектор
в) обратная матрица

Вопрос З**0**. Способ осуществления дешифрования текста при аналитических преобразованиях
а) умножение матрицы на вектор+
б) деление матрицы на вектор
в) перемножение матриц

Лабораторные занятия № 7 -16:

1. Обнаружение вируса и устранение последствий его влияния
2. Установка и настройка антивируса. Настройка обновлений с помощью зеркала
3. Настройка политики безопасности
4. Настройка браузера
5. Работа с реестром
6. Работа с программой восстановления файлов и очистки дисков
7. Измерения в сопровождении программного обеспечения
8. Поэтапное рассмотрение процесса сопровождения: подготовка, анализ проблем и изменений, внесение изменений
9. Работа по сопровождению программного обеспечения, реинжиниринг
10. Работы по модификации: формирование представления об эксплуатируемой/сопровождаемой системе

5.2. Критерии оценивания

5.2.1. Критерии оценивания устного ответа

При оценке устного ответа, обучающегося учитывается:

1) полнота и правильность ответа;
2) степень осознанности, понимания изученного;

Отметка «5»: ответ правильный, полный в соответствии с изученным материалом; материал изложен в определенной логической последовательности, литературным языком.

Отметка «4»: ответ правильный, полный в соответствии с изученным материалом; материал изложен в определенной логической последовательности; возможны отдельные затруднения в формулировке выводов.

Отметка «3»: ответ, в котором в основном правильно, но схематично или с отклонениями от последовательности изложения раскрыт материал или неполный, несвязный ответ, изложенный нелогично

Отметка «2»: при ответе обнаружено непонимание обучающимся основного содержания учебного материала, неумение его анализировать допущены существенные ошибки, которые обучающийся не смог исправить при наводящих вопросах преподавателя, отсутствует логика в изложении материала, нет необходимых обобщений и самостоятельной оценки фактов; недостаточно сформированы навыки устной речи.

5.2.2. Критерии оценивания выполнения заданий на лабораторных и практических занятиях

- **Отметка «5»**: работа выполнена полностью и правильно; сделаны правильные выводы.
- **Отметка «4»**: работа выполнена правильно с учетом 1-2 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.
- **Отметка «3»**: работа выполнена правильно не менее чем на половину или допущены

3-4 существенные ошибки.

- **Отметка «2»**: допущены 5 и более существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя.

Задания к лабораторным занятиям представлены в методических указаниях к лабораторным занятиям по МДК.02.01. Технология разработки программного обеспечения.

Задания к практическим занятиям представлены в методических указаниях к практическим занятиям по МДК.02.01. Технология разработки программного обеспечения.

Методы оценки:

- Защита отчетов по выполненному заданию на практических занятиях.
- Интерпретация результатов наблюдений за деятельностью обучающегося на практических занятиях

5.2.3. Критерии оценивания тестовых заданий

Оценка в баллах	Степень выполнения задания
Неуд.	Выполнено от 0 до 49,9 % предложенных заданий
Удов.	Выполнено от 50 до 69,9% предложенных заданий
Хор.	Выполнено от 70 до 89,9% предложенных заданий
Отл.	Выполнено от 90 до 100% предложенных заданий

5.2.4. Общая классификация ошибок

При оценке знаний и умений учитываются ошибки и недочёты в работе.

Грубыми считаются ошибки:

- незнание определения основных понятий, законов, общепринятых символов обозначений величин;
- неумение выделить в ответе главное; обобщить результаты изучения;
- неумение применить знания для решения задач;
- неумение использовать полученные данные для выводов;
- неумение пользоваться первоисточниками, учебником, справочником;
- нарушение техники безопасности, небрежное отношение к оборудованию

Негрубыми считаются ошибки:

- неточность формулировок, определений, понятий, законов, вызванная неполнотой охвата основных признаков определяемого понятия или заменой 1-3 из этих признаков второстепенными;
- ошибки, вызванные несоблюдением условий проведения лабораторных занятий;
- недостаточно продуманный план устного ответа (нарушение логики изложения, подмена отдельных основных вопросов второстепенными);
- нерациональные методы работы со справочной литературой;
- неумение выполнять лабораторные задания в общем виде.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ МДК 04.02. Обеспечение качества функционирования компьютерных систем

6.1. Теоретические вопросы

1. Понятие ЖЦ ПО. Этапы ЖЦ ПО

2. Понятие качества программных продуктов. Критерии качества
3. Основные аспекты качества программного обеспечения
4. Многоуровневая модель качества программного обеспечения
5. Объекты уязвимости
6. Методы тестирования ПО
7. Дестабилизирующие факторы и угрозы надежности
8. Методы предотвращения угроз надежности
9. Оперативные методы повышения надежности: временная, информационная, программная избыточность
10. Первичные ошибки, вторичные ошибки и их проявления
11. Математические модели описания статистических характеристик ошибок в программах
12. Выявление первичных и вторичных ошибок
13. Анализ рисков и характеристик качества программного обеспечения при внедрении
14. Целесообразность разработки модулей адаптации
15. Методы и средства организационно-правовой защиты информации
16. Методы и средства инженерно-технической защиты информации
17. Вредоносные программы: классификация, методы обнаружения
18. Антивирусные программы: классификация, сравнительный анализ
19. Файрвол: задачи, сравнительный анализ, настройка
20. Типы межсетевых экранов
21. Групповые политики.
22. Аутентификация. Учетные записи
23. Решение проблем конфигурации с помощью групповых политик
24. Управление и обслуживание ИС
25. Средства диагностики оборудования
26. Конфигурирование ИС. Оперативное управление и регламентные работы
27. Тестирование защиты программного обеспечения
28. Основные аспекты компьютерной криптографии
29. Электронная подпись
30. Средства и протоколы шифрования сообщений: AKEP 2 и SKID
31. Средства и протоколы шифрования сообщений: Wide-Mouth Frog и Wide-Mouth Frog
32. Средства и протоколы шифрования сообщений: Средства и протоколы шифрования сообщений: Yahalom и Needham-Schroeder
33. Средства и протоколы шифрования сообщений: Otway-Rees и Neuman-Stubblebine
34. Криптографические механизмы конфиденциальности, целостности и аутентичности информации
35. Криптографические алгоритмы DES и ГОСТ 28147-89
36. Криптографический стандарт DES

6.2. Практические задания

1. Разработка тестовых наборов
2. Разработка руководства пользователя
3. Разработка технического задания

6.3. Критерии оценивания ответов на экзамене

– оценка **«отлично»**, если студент обладает глубокими и прочными знаниями программного материала; при ответе на вопросы продемонстрировал исчерпывающее, последовательное и логически стройное изложение; правильно сформулировал понятия и закономерности по вопросам; сделал вывод по излагаемому материалу;

– оценка **«хорошо»**, если студент обладает достаточно полным знанием программного материала; его ответ представляет грамотное изложение учебного материала; но имеются существенные неточности в формулировании понятий и закономерностей по вопросам; не полностью сделаны выводы по излагаемому материалу;

– оценка **«удовлетворительно»**, если студент имеет общие знания основного материала без усвоения некоторых существенных положений; формулирует основные понятия с некоторой неточностью; затрудняется в приведении примеров, подтверждающих теоретические положения;

– оценка **«неудовлетворительно»**, если студент не знает значительную часть программного материала; допустил существенные ошибки в процессе изложения; не умеет выделить главное и сделать вывод; приводит ошибочные определения; ни один вопрос не рассмотрен до конца, наводящие вопросы не помогают.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

7.1. Основные печатные издания

1. Федорова, Г.И. Разработка, внедрение и адаптация программного обеспечения отраслевой направленности: учебное пособие. – Москва: КУРС, 2021. – 336 с.

7.2. Основные электронные издания

1. Федорова, Г. Н. Разработка, внедрение и адаптация программного обеспечения отраслевой направленности: учебное пособие / Г. Н. Федорова. — Москва: КУРС: ИНФРА-М, 2021. — 336 с. — (Среднее профессиональное образование). - ISBN 978-5-906818-41-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1138896 (дата обращения: 13.12.2021). – Режим доступа: по подписке.

7.3. Дополнительные источники

1. Гвоздева, В. А. Основы построения автоматизированных информационных систем: учебник / В. А. Гвоздева, И. Ю. Лаврентьева. — Москва: ФОРУМ: ИНФРА-М, 2020. — 318 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0705-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/1066509 (дата обращения: 13.12.2021). – Режим доступа: по подписке.
2. От модели объектов - к модели классов. Единое окно доступа к образовательным ресурсам. http://real.tepkom.ru/Real_OM-CM_A.asp