МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.07.02 Сертификация информационных систем

программы подготовки специалистов среднего звена /
квалифицированных рабочих и служащих

09.02.07 Информационные системы и программирование

Форма обучения: *очная*

Находка 2026

Рабочая программа учебной дисциплины *МДК.07.02 Сертификация информационных систем* разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности / профессии *09.02.07 Информационные системы и программирование*, утвержденного приказом Минобрнауки России от «09» декабря 2016 г. № 1547, примерной образовательной программой.

Разработчик(и): *Лихацкий М.Б. преподаватель ОСПО филиала ФГБОУ ВО «ВВГУ» в г. Находке*

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 10 от «29» июня 2026 г.

Председатель ЦМК _____ *В.В Плахотина*
подпись

Содержание

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Место дисциплины в структуре основной образовательной программы

Учебная дисциплина *МДК.07.02 Сертификация информационных систем* является частью учебного цикла основной образовательной программы (далее ООП) в соответствии с ФГОС СПО по специальности/профессии *09.02.07 Информационные системы и программирование.*

1.2 Цель и планируемые результаты освоения дисциплины

По итогам освоения дисциплины, обучающиеся должны продемонстрировать результаты обучения, соотнесённые с результатами освоения ООП СПО, приведенные в таблице.

Код компетенции	Умения	Знания
ОК 1 ОК 2	Обрабатывать нормативную, техническую и текстовую информацию для составления актов сертификационных испытаний, протоколов и заключений о соответствии.	Назначение, виды и нормативно-правовая база сертификации (обязательная и добровольная). Федеральный закон «О техническом регулировании», стандарты серии ГОСТ Р и ИСО.
ОК 4 ОК 5	Применять специализированное программное обеспечение и мультимедийные технологии для оформления комплекта документов (сертификатов, деклараций о соответствии) и схем сертификации.	Состав, структуру, принципы реализации и функционирования систем менеджмента качества (СМК) и систем менеджмента информационной безопасности (СМИБ).
ОК 9 ОК 10	Обрабатывать экономическую и статистическую информацию для расчета затрат на сертификацию, анализа статистики дефектов (построение диаграмм Парето, Исикавы) в пакетах прикладных программ.	Базовые и прикладные информационные технологии; методы и метрики оценки качества программного обеспечения; экономические аспекты лицензирования и сертификации.
ПК 5.1 ПК 5.2 ПК 5.6 ПК 6.3	Собирать исходные данные для проведения сертификационных испытаний. Разрабатывать проектную документацию для подачи в аккредитованные органы по сертификации в соответствии с требованиями заказчика. Разрабатывать подсистемы безопасности информационной системы в соответствии со стандартами безопасности (ГОСТ Р ИСО/МЭК 15408). Производить разработку модулей и проводить их внутреннюю верификацию и тестирование перед сертификацией.	**Инструментальные средства информационных технологий:** методики проведения сертификационных испытаний, средства верификации и аудита (статический анализ кода, нагрузочное тестирование, тестирование на проникновение), а также системы электронного документооборота.

2 Структура и содержание учебной дисциплины

2.1 Объем учебной дисциплины и виды учебной работы

Таблица 2 - Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	46
в том числе:	
– теоретическое обучение	14
– практические занятия *(если предусмотрено)*	30
– самостоятельная работа	
– консультации	
– промежуточная аттестация – *(дифференцируемый зачет)*	2

2.2 Тематический план и содержание учебной дисциплины «МДК.07.02 Сертификация информационных систем»

Таблица 3 - Тематический план дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Тема 1.1 Основы сертификации	**Содержание учебного материала:** Сущность сертификации. Проведение сертификации. Правовые основы сертификации. Организационно-методические принципы сертификации. Действие стандартов серии ИСО в области сертификации. Деятельность МЭК в области сертификации. Международные правовые и нормативные акты обеспечения информационной безопасности процессов переработки информации. Отечественное организационное, правовое и нормативное обеспечении и регулирование в сфере информационной безопасности. Система менеджмента информационной безопасности. Сертификация систем обеспечения качества. Экологическая сертификация. Сертификация информационно-коммуникационных технологий и система ИНКОМТЕХСЕРТ	7	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК 5.1, 5.2, 5.6, ПК 6.3
	Практическое занятие №1: «Анализ нормативно-правовой базы сертификации в РФ» **Практическое занятие №2:** «Разработка технического задания (ТЗ) на сертификацию информационной системы» **Практическое занятие №3:** «Изучение схем сертификации и заполнение заявки на проведение сертификации» **Практическое занятие №4**: «Анализ системы менеджмента качества (СМК) организации»	15	
	Самостоятельная работа обучающихся	Не предусмотрено	
	Лабораторное занятие	Не предусмотрено	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Тема 1.2. Сертификация информационных систем	**Содержание учебного материала:** Объекты информатизации, требующие обязательной сертификации программных средств и обеспечения. Уровни качества программной продукции. Требования к конфигурации серверного оборудования и локальных сетей. Оформление требований. Техническое задание. Системы сертификации. Процедура сертификации. Сертификаты безопасности: виды, функции, срок действия. Проверка наличия сертификата безопасности. Платформы и центры сертификации. Сертификат разработчика. Процесс подписи и проверки кода. SSL сертификат: содержание, формирование запроса, проверка данных с помощью сервисов.	7	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК 5.1, 5.2, 5.6, ПК 6.3
	Практическое занятие №5: «Проверка наличия и подлинности сертификатов безопасности оборудования и программного обеспечения» **Практическое занятие №6:** «Проверка требований к конфигурации серверного оборудования и локальных сетей» **Практическое занятие №7:** «Работа с SSL-сертификатами: формирование запроса, проверка данных с помощью сервисов» **Практическое занятие №8:** «Разработка комплекта документов для проведения процедуры сертификации ПО (Разработка проектной документации)» **Практическое занятие №9:** «Оценка уровня качества и безопасности программного кода (Инструментальные средства)»	15	
	Самостоятельная работа обучающихся	Не предусмотрено	
	Лабораторное занятие	Не предусмотрено	
Промежуточная аттестация - дифференцированный зачет		2	

ИТОГО часов		**46**	
Теоретические занятия		**14**	
Практические занятия		**30**	
Самостоятельная работа		**0**	
Дифференцированный зачет		**2**	

3 Условия реализации учебной дисциплины

3.1 Для реализации программы учебной дисциплины «МДК.07.02 Сертификация информационных систем» образовательной организации, предусмотрено наличие следующих специальных помещений:

Для реализации программы учебной дисциплины предусмотрено наличие следующих специальных помещений:

Компьютерный класс информационных технологий: количество посадочных мест - 28 шт., доска меловая - 1 шт., стол для преподавателя - 1 шт., стул для преподавателя - 1 шт.; учебно-методические пособия, дидактические и презентационные материалы

Компьютерный класс имеет следующее оборудование:
Учебно-лабораторное оборудование: Процессор Intel Количество ядер - 2 . Объем кэш-памяти - 8Мб • Базовая частота процессора - 2,0 ГГц. Объем установленной памяти - 4Гб Накопитель твердотельный объемом 512 видео карта - встроенная. Максимальное разрешение - 1920x1080 пикс. Диагональ монитора 23" количество мониторов 1 шт. Разрешение: FHD (1920x1080 пикс.) клавиатура мышь ОС Microsoft Windows 7 Pro Мультимедийны комплект в составе: проектор Sanyo, крепление Kromax, экран Lumien Eco Picture: Технология проецирования изображения - микрозеркала на полупроводниковом чипе. Базовое разрешение проектора: 1280x800 пикс. Входы - VGA, HDMI 2 шт., Порты - RS-232C, USB 2 шт., LAN Размер полотна: ширина 200 см, высота 127 см.
ПО: Microsoft Office 2010, Пакет Adobe CC 2019, Pixologic Zbrush Academic Volume License, Adobe Substance Painter, Autodesk 3Ds max, Maya, Blender, Unity, Unreal Engine

3.2 Информационное обеспечение реализации программы

Для реализации программы учебной дисциплины библиотечный фонд ВВГУ укомплектован печатными и электронными изданиями.

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Основная литература:

1. Бизяев, А.А. Информационные технологии: практикум: [Электронный ресурс]/А.А. Бизяев, К.А. Куратов ; Новосибирский государственный технический университет. - Новосибирск: Новосибирский государственный технический университет, 2022. - 96 с.: ил., табл. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=575330
2. Информационные технологии [Электронный ресурс] : метод. рекомендации по самостоят. изучению дисциплины / Г.И. Попов, С.И. Бажинов, В.Г. Конюхов, Е.Н. Яшкина, В.А. Пирогов .- М. : РГУФКСМиТ, 2022 .-167 с. : ил. - Режим доступа: https://lib.rucont.ru/efd/671375
3. Информационные технологии в профессиональной деятельности [Электронный ресурс] / Т.В. Марзаева .— Улан-Удэ : Бурятский государственный университет, 2025 .- 71 с. -Режим доступа: https://lib.rucont.ru/efd/348195
4. Информационные технологии: учеб. пособие [Электронный ресурс]/ Л.Г. Гагарина, Я.О. Теплова, Е.Л. Румянцева, А.М. Баин / под ред. Л.Г. Гагариной. — Москва: ИД «ФОРУМ»: ИНФРА- М, 2021. — 320 с. -Режим доступа: https://znanium.com/catalog/product/471464.
5. Филимонова, Е.В. Информационные технологии в профессиональной деятельности : учебник / Филимонова Е.В. — Москва : КноРус, 2022. — 482 с. — (СПО). — ISBN 978-5-406-04887-0. — URL: https://book.ru/book/922139 (дата обращения:

06.08.2024). — Текст : электронный.

6. Хныкина, А.Г. Информационные технологии [Электронный ресурс] : учеб. пособие / Т.В. Минкина, А.Г. Хныкина .— Ставрополь : изд-во СКФУ, 2023 .— 126 с. : ил. — Режим доступа: https://lib.rucont.ru/efd/671178

Дополнительная литература:

1. Богданова, С.В. Информационные технологии [Электронный ресурс]: учебное пособие / С.В. Богданова, А.Н. Ермакова. - Ставрополь: Сервисшкола, 2024. - 211 с. - Режим доступа: https://znanium.com/catalog/product/514867

2. Самойленко, А.П. Информационные технологии статистической обработки данных [Электронный ресурс] : учеб. пособие / О.А. Усенко, Южный федеральный ун-т, А.П. Самойленко .— Ростов н/Д. : Изд-во ЮФУ, 2024 .— 128 с. : ил. — ISBN 978-5-9275-2521-8 .— Режим доступа: https://lib.rucont.ru/efd/692393

3. Суханова, О.Н. Информационные технологии [Электронный ресурс] : лаб. практикум / О.В.

4. Ментюкова, О.Н. Суханова .— Пенза : РИО ПГСХА, 2022 .- 116 с. : ил. - Режим доступа: https://lib.rucont.ru/efd/323727.

Интернет-ресурсы:

1. www.informatics.mccme.ru/moodle/ - дистанционная подготовка по информатике.
2. www.ixbt.com - сайт о высоких технологиях, новости индустрии из мира компьютерного «железа», тестовые испытания и обзоры оборудования. Конференция. Платформа ПК. Цифровой звук. Цифровое фото. Мобильные устройства. Форум.
3. www.lib.ru/INTERMET/termwww.txt - толковый словарь терминов.
4. www.computerra.ru - новости про компьютеры, железо, новые технологии, информационные технологии. Рубрики: В поле зрения; Компьютерралаб; Дюжина полезных программ; Реклама на сайте; Блоги; Наука и жизнь. Архив номеров журнала.
5. www.novtex.ru/IT/arhiv.htm
6. https://www.planttext.com/
7. https://kroki.io/#
8. https://www.canva.com/ru ru/
9. https://prezi.com/
10. www.jip.ru/ - электронный научный журнал.

4. Контроль результатов освоения учебной дисциплины

Результаты обучения	Критерии оценки	Методы оценки
- 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 - основные методы и средства сбора, обработки, хранения, передачи и накопления информации; - технологию поиска информации в сети Интернет; - номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; - формат оформления результатов поиска информации - содержание актуальной нормативно-правовой документации;	Уровень правильных ответов при письменном и устном контроле, четкость изложения материала. Быстрота ориентации в представляемом материале, быстрота реакции на вопросы. Правильность, полнота выполнения заданий, точность формулировок, точность расчетов, соответствие требованиям.	устный опрос, практические работы

- современная научная и профессиональная терминология; - возможные траектории профессионального развития и самообразования - психологические основы деятельности коллектива, психологические особенности личности; - основы проектной деятельности - особенности социального и культурного контекста; - правила оформления документов и построения устных сообщений - назначение, состав, основные характеристики организационной и компьютерной техники;		
- основные компоненты информационных систем, принципы внедрения информационных систем, организацию межсетевого взаимодействия; - назначение и принципы использования системного и прикладного программного обеспечения; - принципы защиты информации от несанкционированного доступа; - правовые аспекты использования информационных технологий и программного обеспечения; - основные понятия	Оптимальность выбора способов действий, методов, последовательностей действий. Соответствие требованиям инструкций, регламентов, рациональность действий. Точность распознавания проблемных ситуаций в различных контекстах; Адекватность анализа сложных ситуаций при решении задач профессиональной деятельности, эффективность поиска. Точность определения источников нужных ресурсов. Разработка детального плана действий, правильность оценки рисков на каждом шагу; Точность оценки плюсов и минусов полученного результата, своего плана и его реализации, предложение критериев оценки и рекомендаций по улучшению плана	Текущий контроль: экспертное наблюдение и оценка в процессе выполнения заданий для практических занятий;

автоматизированной обработки информации;		

Для оценки достижения запланированных результатов обучения по дисциплине разработаны контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации, которые прилагаются к рабочей программе дисциплины.

Для оценки достижения запланированных результатов обучения по дисциплине разработаны контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации, которые прилагаются к рабочей программе дисциплины.

Оценка результатов обучения производится при помощи бально-рейтинговой системы.

Основные критерии оценки:

- конспектирование 0,5 баллов;
- активность на уроке 0,5 баллов;
- посещаемость занятий 0,5 баллов;
- выполнение индивидуальных домашних заданий 1 задание- 1 балл;
- выполнение самостоятельной работы 1 балл;
- лабораторная работа 3 балла;
- контрольная работа 1 задание -1 балл;
- участие в научно-исследовательской работе 15 баллов;
- дифференцированный зачет 20 баллов.

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине

«МДК.07.02 Сертификация информационных систем»
программы подготовки специалистов среднего звена /
квалифицированных рабочих и служащих

09.02.07 Информационные системы и программирование

Форма обучения: ***очная***

Находка 2026

Оценочные средства для проведения текущего контроля и промежуточной аттестации по учебной дисциплине *«МДК.07.02 Сертификация информационных систем»* разработаны в соответствии с требованиями ФГОС СПО по специальности / профессии *09.02.07 Информационные системы и программирование*, утвержденного приказом Минобрнауки России от «09» декабря 2016 г. № 1547, примерной образовательной программой.

Разработчик(и): *Лихацкий М.Б. преподаватель ОСПО филиала ФГБОУ ВО «ВВГУ» в г. Находке*

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 10 от «29» июня 2026 г.

Председатель ЦМК _____ *В.В Плахотина*

подпись

1 Общие сведения

Фонд оценочных средств (далее – ФОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины *«МДК.07.02 Сертификация информационных систем»* ФОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта (с использованием оценочного средства - *тестирование*)

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК	Код результата обучения	Наименование результата обучения[1]
ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.1 ПК 5.2 ПК 5.6 ПК 6.3	З1	Знать нормативно-правовую базу сертификации (ФЗ «О техническом регулировании», ГОСТ Р, ISO), виды и схемы обязательной и добровольной сертификации.
	З2	Знать состав, структуру и принципы функционирования систем менеджмента качества (СМК) и систем менеджмента информационной безопасности (СМИБ), а также требования к оформлению сертификатов и деклараций.
	З3	Знать методы оценки качества, метрики и экономические аспекты сертификации (расчет затрат, лицензирование).
	З4	Знать инструментальные средства, методики проведения сертификационных испытаний и аудита (тестирование на проникновение, статический анализ кода, проверка SSL-сертификатов), а также требования стандартов ГОСТ 34, ГОСТ Р ИСО/МЭК 15408.
	У1	Уметь собирать исходные данные, обрабатывать нормативную и техническую информацию для составления актов испытаний, протоколов и заключений о соответствии.
	У2	Уметь применять специализированное ПО для оформления комплекта документов (сертификатов, деклараций) и проведения анализа сертификатов безопасности (в том числе SSL-сертификатов).
	У3	Уметь обрабатывать экономическую и статистическую информацию, рассчитывать стоимость сертификации и анализировать статистику дефектов (инструменты качества: Парето, Исикава).

3 Соответствие оценочных средств контролируемым результатам обучения

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель[2] овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
1. Введение в ИТ				
Тема 1.1 Основы сертификации	З1	Способность понимать нормативно-правовую базу сертификации (ФЗ «О техническом регулировании», стандарты ГОСТ Р и ISO).	*Устный опрос (п 5.1 вопросы 1-7)* *Реферат (п 5.2 темы 1-12)* *Практическая работа №1-4 (п 5.3)*	*Устный опрос (п 6.1 вопросы 1-15)* *Тест вариант №1-2 (п 6.2)*
	З2	Способность изучать состав, структуру и принципы функционирования систем менеджмента качества (СМК) и системы менеджмента информационной безопасности (СМИБ).		
	У1	Способность собирать исходные данные и разрабатывать заявку на проведение сертификации, а также оформлять акты и протоколы испытаний.		
Тема 1.2. Сертификация информационных систем	З3	Способность знать виды сертификатов безопасности (включая SSL), требования к конфигурации серверного оборудования и методики проверки подлинности.	*Устный опрос (п 5.1 вопросы 8-15)* *Реферат (п 5.2 темы 13-30)* *Практическая работа №5-9 (п 5.3)*	*Устный опрос (п 6.1 вопросы 1-18)* *Тест вариант №1-2 (п 6.2)*
	У2	Способность применять специализированное ПО для проверки наличия и подлинности сертификатов, а также формирования запросов на сертификаты.		
	У3	Способность обрабатывать экономическую и статистическую информацию для расчета затрат на сертификацию и анализа качества.		
	У4	Способность производить разработку модулей и проводить внутреннюю верификацию перед сертификацией в соответствии с техническим заданием.		

4. Описание процедуры оценивания

Результаты обучения по дисциплине, уровень сформированности компетенций оцениваются по четырёх бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по дисциплине проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом. *Оценка на зачете выставляется с учетом оценок, полученных при прохождении текущей аттестации*.

Критерии оценивания устного ответа

(оценочные средства: *собеседование, устное сообщение)*

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

(оценочные средства: *реферат, конспект, контрольная работа, расчетно-графическая работа, доклад (сообщение), в том числе выполненный в форме презентации, творческое задание*).

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена

правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

Оценка	*Отлично*	*Хорошо*	*Удовлетворительно*	*Неудовлетворительно*
Количество правильных ответов	91 % и ≥	от 81% до 90,9 %	не менее 70%	менее 70%

Критерии выставления оценки студенту на зачете

(оценочные средства: *устный опрос в форме ответов на вопросы билетов, устный опрос в форме собеседования, выполнение письменных разноуровневых задач и заданий, комплексная расчетно-графическая работа, творческое задание, кейс-задача, портфолио, проект и т.п.)*

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения

	логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для устного опроса

1. Дайте определение сертификации. Какова её основная цель?
2. Чем отличается обязательная сертификация от добровольной? Приведите примеры продукции, для которых сертификация является обязательной.
3. Назовите основных участников процесса сертификации. Какую роль выполняет орган по сертификации?
4. Что такое сертификат соответствия и каков его срок действия?
5. Опишите типичные этапы процедуры сертификации продукции.
6. Что такое «знак соответствия» и для чего он применяется?
7. Что такое схема сертификации? Кем она устанавливается?
8. Что такое инспекционный контроль и какова его цель в процессе сертификации?
9. Какие виды объектов могут подвергаться сертификации (продукция, системы, персонал)?
10. Назовите основные российские органы исполнительной власти, участвующие в сертификации в сфере ИТ и защиты информации.
    Что понимается под сертификацией информационных систем (ИС)? Какие её цели?
11. Назовите основные направления или аспекты ИС, которые проверяются в процессе её сертификации.
12. Какие классы стандартов используются для оценки безопасности информационных технологий? Что вы знаете о стандарте Common Criteria (ISO/IEC 15408)?
13. Что такое «Уровень доверия к безопасности» (EAL) в рамках Common Criteria? На что влияет его значение?
14. С какими целями проводится обязательная сертификация информационных систем в России?
15. Какие российские нормативные акты и стандарты регулируют требования к защите информации в ИС (например, при обработке персональных данных)?

5.2 Темы рефератов

Тема 1.1. Основы сертификации

1. Сущность сертификации информационных систем и ее место в системе обеспечения качества.

2. Правовые основы сертификации в РФ: Федеральный закон «О техническом регулировании».

3. Организационно-методические принципы проведения сертификации в РФ.

4. Деятельность стандартов серии ИСО в области сертификации и их роль.

5. Международные правовые и нормативные акты, обеспечивающие информационную безопасность.

6. Отечественное организационное, правовое и нормативное обеспечение в сфере информационной безопасности.

7. Система менеджмента информационной безопасности (СМИБ): структура и принципы функционирования.

8. Система менеджмента качества (СМК) как основа для сертификации предприятия.

9. Экологическая сертификация и ее влияние на деятельность ИТ-организаций.

10. Сертификация информационно-коммуникационных технологий: особенности и перспективы.

11. Система сертификации ИНКОМТЕКСЕРТ: история, принципы и область деятельности.

12. Сравнительный анализ обязательной и добровольной сертификации в сфере ИТ.

Тема 1.2. Сертификация информационных систем

13. Объекты информатизации, требующие обязательной сертификации программных средств.

14. Уровни качества программной продукции и требования к ним при сертификации.

15. Требования к конфигурации серверного оборудования и локальных сетей при сертификации.

16. Порядок разработки и оформления технического задания (ТЗ) на сертификацию.

17. Системы сертификации и процедура их проведения: этапы и участники.

18. Сертификаты безопасности: виды, функции, сроки действия и порядок получения.

19. Платформы и центры сертификации: их роль в системе обеспечения доверия.

20. Сертификат разработчика: процесс подписи и проверки кода (Code Signing).

21. SSL-сертификат: содержание, формирование запроса и проверка данных с помощью сервисов.

22. Методика проверки наличия и подлинности сертификатов безопасности оборудования.

23. Анализ и оценка уровня качества и безопасности программного кода (инструментальные средства).

24. Разработка комплекта документов для проведения процедуры сертификации ПО (проектная документация).

25. Роль аккредитованных испытательных лабораторий в процессе сертификации ИС.

26. Международные стандарты ISO/IEC 15408 (Common Criteria) и их применение при

сертификации.

27. Сертификация систем менеджмента качества (ISO 9001) как необходимое условие для производства качественного ПО.

28. Процесс аккредитации органов по сертификации и его значение для рынка ИТ.

29. Особенности сертификации средств криптографической защиты информации (СКЗИ).

30. Экономические аспекты сертификации: расчет затрат и оценка эффективности.

6. Оценочные средства для проведения промежуточной аттестации

6.1 Вопросы для собеседования при проведении дифференцированного зачета

Тема 1.1. Основы сертификации

1. **Что такое сертификация информационных систем?** В чем разница между обязательной и добровольной сертификацией?
2. **Какие нормативно-правовые акты регулируют процесс сертификации в РФ?** Назовите основные законы (например, ФЗ «О техническом регулировании») и стандарты (ГОСТ Р, ISO).
3. **Что такое Система менеджмента качества (СМК)?** Какие стандарты серии ISO (например, ISO 9001) регулируют требования к СМК?
4. **Что такое Система менеджмента информационной безопасности (СМИБ)?** Какой стандарт (ISO/IEC 27001) регламентирует требования к ней?
5. **Опишите основные этапы процедуры сертификации программного продукта** от подачи заявки до получения сертификата.
6. **Что такое «схема сертификации»?** Приведите примеры схем (1с, 3с, 5с) и объясните, чем они отличаются.
7. **Какие функции выполняют аккредитованные органы по сертификации и испытательные лаборатории?** Какую роль играет Росаккредитация?

Тема 1.2. Сертификация информационных систем

8. **Какие объекты подлежат обязательной сертификации в области ИТ?** Приведите примеры (криптографические средства, средства защиты информации, ПО для гос. нужд).
9. **Что такое сертификат безопасности (в том числе SSL-сертификат)?** Назовите их основные виды (DV, OV, EV) и укажите отличия в уровне проверки.
10. **Как проверить подлинность SSL-сертификата?** Опишите алгоритм действий с использованием онлайн-сервисов (например, SSL Labs) или встроенных средств браузера.
11. **Опишите процесс формирования запроса на SSL-сертификат (CSR).** Какие данные необходимо указать и куда отправляется запрос?
12. **Что такое «центр сертификации» (Certificate Authority, CA)?** Опишите процесс выпуска, подписи и проверки кода (Code Signing).
13. **Какие требования предъявляются к конфигурации серверного оборудования и локальных сетей при подготовке к сертификации?** Опишите основные параметры (разграничение прав, протоколы, защита каналов).
14. **Что такое техническое задание (ТЗ) на проведение сертификации?** Какие исходные данные в нем должны быть указаны?
15. **Как производится оценка качества программного продукта перед сертификацией?** Опишите основные метрики и методы (например, нагрузочное тестирование, статический анализ кода).

5.3 Примеры практических работ

Практическое занятие №1: Анализ нормативно-правовой базы сертификации в РФ
Цель: Изучить законодательную базу в области сертификации, научиться находить нужные стандарты.
Задание: Провести анализ нормативных документов и заполнить таблицу.
Пример выполнения (для отчета):

Документ	Что регулирует
ФЗ «О техническом регулировании»	Основные принципы обязательной и добровольной сертификации, виды схем.
ФЗ «О персональных данных»	Требования к защите ПДн в информационных системах.
ГОСТ Р ИСО 9001	Требования к системам менеджмента качества (СМК) предприятия.
ГОСТ Р ИСО/МЭК 15408 (Common Criteria)	Критерии оценки безопасности информационных технологий.
Результат: Таблица со ссылками на конкретные статьи или разделы стандартов.	

Практическое занятие №2: Разработка и оформление технического задания (ТЗ) на сертификацию информационной системы
Цель: Отработать навык сбора исходных данных и составления профессиональной документации (закрывает ПК 5.1 и 5.2).
Задание: Составить макет ТЗ на сертификацию условной ИС (например, «Интернет-магазин»).
Пример выполнения:

1. **Общие сведения:** ИС «Магазин». Заказчик: ООО «Ромашка».

2. **Цель сертификации:** Подтверждение соответствия требованиям безопасности информации.

3. **Требования к ИС:** Перечень проверяемых функций, требования к среде функционирования.

4. **Состав испытаний:** Функциональное тестирование, проверка защиты от несанкционированного доступа, проверка резервного копирования.
   Результат: Готовый документ на 3-5 страниц.

Практическое занятие №3: Изучение схем сертификации и заполнение заявки на проведение сертификации
Цель: Научиться выбирать схему сертификации и оформлять заявку.
Задание: Определить наиболее подходящую схему для сложного программного обеспечения.
Пример выполнения: Для сложного ПО (например, СУБД) выбирается **Схема 5с** (сертификация системы менеджмента качества производителя и испытания партии). Для простого ПО — **Схема 1с** (испытания типа).
Результат: Заполненный шаблон официальной заявки с выбранной схемой и обоснованием выбора.

Практическое занятие №4: Анализ системы менеджмента качества (СМК) организации

Цель: Оценить готовность предприятия к сертификации по стандарту ISO 9001.
Задание: Проанализировать эталонную структуру СМК предприятия.
Пример выполнения: Студент описывает политику в области качества, документированные процедуры, перечень обязательных записей (протоколы, отчеты), а также делает вывод о соответствии. В выводе указываются несоответствия (например, отсутствие регулярной оценки удовлетворенности клиентов).
Результат: Аналитический отчет с выводами.

Тема 1.2. Сертификация информационных систем

Практическое занятие №5: Проверка наличия и подлинности сертификатов безопасности оборудования и программного обеспечения
Цель: Научиться работать с реестрами Росаккредитации и ФСТЭК.
Задание: Проверить наличие сертификатов на популярные продукты (Windows, Kaspersky, MySQL и др.).
Пример выполнения: Студент заходит на официальные сайты (fstec.ru, pub.fstec.ru), ищет сертификат на конкретный продукт, выписывает его номер и срок действия. Заполняет таблицу: *Наименование ПО | Сертификат № | Орган, выдавший | Срок действия*.
Результат: Заполненная таблица с выводами о наличии/отсутствии сертификатов.

Практическое занятие №6: Проверка требований к конфигурации серверного оборудования и локальных сетей
Цель: Отработать навыки аудита сетевой инфраструктуры.
Задание: Провести аудит условной ЛВС на соответствие требованиям безопасности.
Пример выполнения: Студент описывает схему сети, проверяет наличие межсетевого экрана, физическое разграничение сегментов, сложность паролей, использование шифрования, наличие резервного копирования. По результатам пишет **Акт проверки** с выявленными несоответствиями (например, пароль администратора "12345").
Результат: Акт с рекомендациями по исправлению несоответствий.

Практическое занятие №7: Работа с SSL-сертификатами: формирование запроса, проверка данных с помощью сервисов
Цель: Научиться генерировать CSR и проверять сертификаты сайтов.
Задание: Создать запрос на сертификат и проверить реальный сайт.
Пример выполнения:

1. **Формирование запроса:** Студент использует OpenSSL или онлайн-генератор (например, sslshopper.com) и создает приватный ключ + файл CSR (с указанием домена и организации). Копирует текст запроса в отчет.

2. **Проверка реального сайта:** Студент заходит на сайт **ssllabs.com**, вводит адрес любого крупного сайта (например, sberbank.ru), анализирует рейтинг (A+ или C), срок действия, наличие ошибок.
   Результат: Скриншоты работы и подробный анализ в отчете.

Практическое занятие №8: Разработка комплекта документов для проведения процедуры сертификации ПО (Разработка проектной документации)
Цель: Подготовить полный пакет документов (закрывает ПК 5.2).
Задание: Создать шаблоны документов для подачи на сертификацию условного ПО.
Пример выполнения: Студенту дается исходная спецификация. Он готовит (по шаблонам):

- **Описание программы** (назначение, область применения, функциональные характеристики);

- **Руководство пользователя** (краткая инструкция);

- **Программа и методика испытаний** (сценарий тестирования);

- **Заявку и анкету**.
  Результат: Комплект из 4-5 файлов, объединенных в папку.

Практическое занятие №9: Оценка уровня качества и безопасности программного кода (Инструментальные средства)
Цель: Освоить инструменты статического анализа кода и метрики (закрывает ПК 5.6 и 6.3).
Задание: Проанализировать предоставленный фрагмент кода.
Пример выполнения: Студент запускает бесплатный анализатор (например, **SonarQube** или **PVS-Studio** в ознакомительном режиме) на простом коде.

1. Выявляет уязвимости (например, SQL-инъекция, незакрытые скобки).

2. Рассчитывает метрики (количество строк, цикломатическая сложность).

3. Пишет краткое **Заключение о качестве**: «Обнаружены ошибки типа X и Y, код требует рефакторинга и дополнительной защиты перед подачей на сертификацию».
   Результат: Отчет с перечнем найденных уязвимостей и оценкой уровня безопасности.

6.2 Тестовые материалы

Вариант 1

Часть 1. Выбор одного правильного ответа (вопросы 1–3)

1. Каким федеральным законом регулируются основные принципы обязательной и добровольной сертификации в РФ?
   А) ФЗ «О техническом регулировании»
   Б) ФЗ «О персональных данных»
   В) ФЗ «Об информации, информационных технологиях и о защите информации»
   Г) ФЗ «О сертификации продукции»
2. Что такое SSL-сертификат?
   А) Документ, подтверждающий качество программного кода
   Б) Сертификат безопасности, устанавливающий защищенное соединение и подтверждающий подлинность сайта
   В) Сертификат, подтверждающий соответствие системы менеджмента качества
   Г) Лицензия на использование программного обеспечения
3. Какую функцию выполняет Росаккредитация в системе сертификации?
   А) Проводит испытания продукции
   Б) Выдает сертификаты заявителям
   В) Осуществляет надзор за деятельностью органов по сертификации и лабораторий
   Г) Разрабатывает технические регламенты

Часть 2. Установление соответствия (вопросы 4–6)

4. Установите соответствие между стандартом и его назначением.
   Стандарт: 1. ISO 9001, 2. ISO/IEC 15408 (Common Criteria), 3. ISO/IEC 27001

Назначение: А. Система менеджмента информационной безопасности, Б. Система менеджмента качества, В. Критерии оценки безопасности информационных технологий.

5. Установите соответствие между участником процесса сертификации и его функцией.
   Участник: 1. Заявитель, 2. Орган по сертификации, 3. Испытательная лаборатория
   Функция: А. Проводит испытания образцов, Б. Принимает и анализирует заявку, выдает сертификат, В. Подает заявку и предоставляет документацию на продукцию.

6. Установите соответствие между типом SSL-сертификата и уровнем проверки.
   Тип: 1. DV (Domain Validation), 2. OV (Organization Validation), 3. EV (Extended Validation)
   Уровень: А. Проверка только доменного имени, Б. Проверка организации и домена, В. Расширенная проверка, включающая юридический статус компании (самый высокий уровень доверия).

Часть 3. Установление последовательности (вопросы 7–9)

7. Расставьте в правильной последовательности этапы процедуры сертификации продукции:
   1. Проведение испытаний в лаборатории
   2. Принятие решения о выдаче сертификата
   3. Подача заявки в орган по сертификации
   4. Анализ предоставленной документации
   5. Оформление и выдача сертификата

8. Расставьте в правильном порядке процесс получения SSL-сертификата:
   1. Отправка запроса (CSR) в удостоверяющий центр
   2. Проверка данных удостоверяющим центром
   3. Формирование запроса на сертификат (CSR) на сервере
   4. Выпуск сертификата и его установка на сервер

9. Расставьте в правильной последовательности действия разработчика перед сертификацией программного модуля:
   1. Проведение внутреннего тестирования и отладки
   2. Анализ требований технического задания (ТЗ)
   3. Проведение статического анализа кода на уязвимости
   4. Передача модуля в аккредитованную лабораторию

Часть 4. Открытые вопросы (вопросы 10–12)

10. В чем заключается разница между обязательной и добровольной сертификацией? Приведите примеры объектов обязательной сертификации в сфере ИТ.
11. Что такое «схема сертификации»? Кем она устанавливается и что определяет?
12. Что такое уровень доверия к безопасности (EAL) в стандарте Common Criteria? На что влияет его значение?

Вариант 2

Часть 1. Выбор одного правильного ответа (вопросы 1–3)

1. Какой объект в сфере информационных технологий подлежит обязательной сертификации?
   А) Любой сайт в сети Интернет
   Б) Средства криптографической защиты информации (СКЗИ) и средства защиты государственных информационных систем
   В) Программное обеспечение для развлечений
   Г) Мобильные приложения частных разработчиков

2. Что такое Удостоверяющий центр (Certificate Authority, CA)?
   А) Организация, которая проводит тестирование программного обеспечения
   Б) Организация, которая выпускает и подписывает цифровые сертификаты
   В) Отдел разработки ИТ-компании
   Г) Государственный орган, выдающий лицензии
3. Какова главная цель инспекционного контроля при сертификации?
   А) Первичная проверка качества продукции
   Б) Периодическая проверка, чтобы убедиться, что качество сертифицированной продукции не ухудшилось
   В) Оценка квалификации персонала предприятия
   Г) Выдача нового сертификата

Часть 2. Установление соответствия (вопросы 4–6)

4. Установите соответствие между понятием и его определением.
   Понятие: 1. Сертификат соответствия, 2. Знак соответствия, 3. Декларация соответствия
   Определение: А. Маркировка на продукции, подтверждающая успешное прохождение сертификации, Б. Документ, выданный органом по сертификации, подтверждающий соответствие требованиям, В. Документ, в котором производитель сам заявляет о соответствии продукции требованиям.

5. Установите соответствие между этапом и его действием в рамках аудита ИС.
   Этап: 1. Анализ требований, 2. Проверка конфигурации сети, 3. Оценка защищенности кода
   Действие: А. Проверка межсетевых экранов и разграничения прав доступа, Б. Изучение технического задания и стандартов, В. Поиск уязвимостей (например, SQL-инъекций) с помощью статического анализа.

6. Установите соответствие между объектом сертификации и примером.
   Объект: 1. Продукция, 2. Система, 3. Персонал
   Пример: А. Программный комплекс для автоматизации склада, Б. Система менеджмента качества предприятия, В. Квалификация специалиста по защите информации.

Часть 3. Установление последовательности (вопросы 7–9)

7. Расставьте в правильной последовательности проверку SSL-сертификата на сайте:
   1. Проверка срока действия сертификата
   2. Открытие браузера и переход на защищенный сайт
   3. Просмотр цепочки доверия (выпущен ли сертификат доверенным центром)
   4. Нажатие на значок замка в адресной строке для просмотра деталей

8. Расставьте в правильной последовательности этапы разработки ИС перед подачей на сертификацию:
   1. Разработка модулей в соответствии с ТЗ
   2. Сбор исходных данных и требований заказчика
   3. Проведение верификации (внутренней проверки) и тестирования
   4. Оформление технического задания (ТЗ)

9. Расставьте в правильной последовательности работы по оценке безопасности программного кода:
   1. Составление отчета о найденных уязвимостях
   2. Динамическое тестирование (запуск программы с негативными сценариями)
   3. Статический анализ исходного кода
   4. Устранение найденных ошибок разработчиком

Часть 4. Открытые вопросы (вопросы 10–12)

10. Назовите основные российские органы исполнительной власти, участвующие в сертификации в сфере ИТ и защиты информации.
11. Что понимается под сертификацией информационных систем (ИС) и какие основные аспекты ИС проверяются в процессе её сертификации?
12. Что такое Система менеджмента качества (СМК)? Назовите основной стандарт, регламентирующий требования к ней.

6.3 Ключи к тестовым заданиям для проведения промежуточной аттестации

Вариант 1:

1. **А**
2. **Б**
3. **В**
4. **1-Б, 2-В, 3-А**
5. **1-В, 2-Б, 3-А**
6. **1-А, 2-Б, 3-В**
7. **3, 4, 1, 2, 5**
8. **3, 1, 2, 4**
9. **2, 1, 3, 4**
10. *Модель ответа:* Обязательная сертификация устанавливается законом и обязательна для продукции, влияющей на безопасность (СКЗИ, защита гос. ИС). Добровольная проводится по инициативе производителя для повышения конкурентоспособности.
11. *Модель ответа:* Схема сертификации — это совокупность правил и процедур (испытания типа, анализ производства, сертификация СМК), устанавливается в техрегламентах или владельцем системы сертификации. Определяет объем испытаний.
12. *Модель ответа:* EAL (Evaluation Assurance Level) — это уровень гарантии/строгости оценки безопасности от 1 до 7. Чем выше уровень, тем тщательнее и глубже проводились проверки и тем выше доверие к защищенности продукта.

Ответ может быть сформулирован в другой близкой по смыслу формулировке

Вариант 2:

1. **Б**
2. **Б**
3. **Б**
4. **1-Б, 2-А, 3-В**
5. **1-Б, 2-А, 3-В**
6. **1-А, 2-Б, 3-В**
7. **2, 4, 3, 1**
8. **2, 4, 1, 3**
9. **3, 2, 1, 4**
10. *Модель ответа:* Росстандарт, ФСТЭК России (средства защиты информации), ФСБ России (криптография), Росаккредитация (надзор и аккредитация).
11. *Модель ответа:* Сертификация ИС — это подтверждение соответствия системы требованиям безопасности (ИБ). Проверяются: архитектура, конфигурация серверов и сетей, политика разграничения доступа, защита данных, уровень кода, а также документация.
12. *Модель ответа:* СМК — это совокупность организационных процессов, методов и ресурсов, направленных на управление качеством. Основной международный стандарт — ISO 9001.

Ответ может быть сформулирован в другой близкой по смыслу формулировке

6.4 Ключи к вопросам для собеседования при проведении дифференцированного зачета

- **Вопрос 1:** *Сертификация* — процедура подтверждения соответствия продукции установленным требованиям. *Обязательная* — по закону (например, для средств защиты информации), *добровольная* — по инициативе производителя для повышения конкурентоспособности.
- **Вопрос 2:** ФЗ «О техническом регулировании», ФЗ «Об информации, информационных технологиях и о защите информации», ГОСТ Р 50922 (защита информации), стандарты ISO/IEC 15408 (критерии оценки безопасности ИТ), ISO 9001 (качество).
- **Вопрос 3:** СМК — это совокупность организационной структуры, процессов и ресурсов для управления качеством. Стандарт ISO 9001 является основным для подтверждения, что процессы разработки соответствуют требованиям качества.
- **Вопрос 4:** СМИБ — это часть общей системы управления предприятием, направленная на защиту информации. Стандарт ISO/IEC 27001 определяет требования к рискам, политикам безопасности и контролю доступа.
- **Вопрос 5:** 1) Подача заявки в аккредитованный орган; 2) Идентификация и анализ ТЗ; 3) Проведение сертификационных испытаний (тестов); 4) Анализ протоколов испытаний; 5) Оформление и выдача сертификата соответствия; 6) Инспекционный контроль (периодическая проверка).
- **Вопрос 6:** Схема определяет порядок и объем испытаний. Например, схема 1с — испытания образца заявителем, схема 3с — испытания аккредитованной лабораторией, схема 5с — сертификация системы качества производителя.
- **Вопрос 7:** *Орган по сертификации* — принимает решения о выдаче сертификатов, оформляет их. *Испытательные лаборатории* — проводят физические и программные испытания. *Росаккредитация* — осуществляет надзор за деятельностью органов и лабораторий.
- **Вопрос 8:** Под обязательную сертификацию попадают: средства криптографической защиты информации (СКЗИ), средства защиты от несанкционированного доступа, программное обеспечение для государственных информационных систем (ГИС).
- **Вопрос 9:** SSL-сертификат — цифровая подпись для шифрования трафика и подтверждения подлинности сайта. *DV* (Domain Validation) — проверка домена, *OV* (Organization Validation) — проверка организации, *EV* (Extended Validation) — расширенная проверка (высший уровень доверия).
- **Вопрос 10:** Проверка подлинности выполняется по «цепочке доверия»: 1) браузер сверяет сертификат с доверенными корневыми сертификатами; 2) сервисы типа SSL Labs проверяют срок действия, правильность цепочки и наличие ошибок в конфигурации.
- **Вопрос 11:** CSR (Certificate Signing Request) создается на сервере (в панели управления или через OpenSSL). В него входит: публичный ключ, доменное имя, информация об организации. Запрос отправляется в удостоверяющий центр (CA).
- **Вопрос 12:** CA (например, ИНКОМТЕКСЕРТ) — это доверенная организация, которая подписывает сертификаты своим закрытым ключом. Выпущенный сертификат используется для подписи кода (Code Signing) и защиты веб-трафика. Проверка кода осуществляется через его цифровую подпись.
- **Вопрос 13:** Требования: использование Firewall для разделения сетей, применение протоколов шифрования (TLS), настройка сложных паролей и политик их смены, разделение ролей (администратор/пользователь), установка антивирусного ПО.
- **Вопрос 14:** ТЗ на сертификацию содержит: описание назначения системы, перечень проверяемых функций, технические характеристики, требования к безопасности, методики испытаний и критерии оценки результатов.
- **Вопрос 15:** Оценка производится с помощью метрик: плотность дефектов, покрытие кода. Методы: статический анализ (ищет уязвимости в коде), динамическое тестирование (проверка поведения).

Все ответы могут быть сформулированы в другой близкой по смыслу формулировке

6.5 Ключи на вопросы для устного опроса

1. Определение сертификации и её цель

Сертификация — это процедура подтверждения соответствия продукции, процессов или услуг установленным требованиям, нормативным документам и стандартам . Основная цель — защита потребителя от некачественной продукции и обеспечение безопасности, а также повышение доверия между участниками рынка.

2. Обязательная и добровольная сертификация

- **Обязательная сертификация** устанавливается законом и подтверждает соответствие требованиям безопасности (например, для средств защиты информации, криптографии, систем, используемых в госорганах) .
- **Добровольная сертификация** проводится по инициативе производителя для подтверждения качества и повышения конкурентоспособности. В сфере ИТ это часто используется в тендерах и для работы с крупными клиентами (например, в системе «Росинфосерт») .

3. Участники процесса и роль органа по сертификации

Ключевые участники: заявитель (производитель), орган по сертификации и аккредитованная испытательная лаборатория .

Роль органа по сертификации: он проводит экспертизу документов, контролирует испытания, оформляет и выдает сертификаты, а также осуществляет надзор за уже выданными документами .

4. Сертификат соответствия и его срок действия

Сертификат соответствия — это официальный документ, подтверждающий, что продукция или система отвечает требованиям стандартов. Срок действия определяется выбранной схемой сертификации и действует в течение всего периода, пока продукция сохраняет заявленные характеристики .

5. Типичные этапы процедуры сертификации

1. Подача заявки в орган по сертификации.
2. Анализ технической документации и требований.
3. Отбор образцов и проведение испытаний в лаборатории.
4. Анализ состояния производства (при необходимости).
5. Принятие решения о выдаче сертификата.
6. Оформление и выдача документа, внесение в реестр .

6. Знак соответствия

Знак соответствия — это маркировка, подтверждающая, что продукция прошла сертификацию в конкретной системе (например, знак обращения на рынке). Он используется для маркировки упаковки и рекламных материалов, что помогает потребителю визуально идентифицировать подтверждение качества .

7. Схема сертификации

Схема — это набор процедур и правил, определяющих, как именно будет проводиться оценка соответствия (например, испытания типа, анализ производства, контроль системы менеджмента). Она устанавливается владельцем системы сертификации или техническим регламентом .

8. Инспекционный контроль

Это периодическая проверка сертифицированной продукции в течение всего срока действия сертификата. Цель — убедиться, что качество не ухудшилось. По результатам контроля орган может подтвердить действие сертификата, приостановить его или полностью отменить .

9. Виды объектов сертификации

Сертифицировать можно практически любые объекты: готовую продукцию (оборудование, ПО), системы менеджмента (например, ISO 27001), услуги, а также квалификацию персонала.

10. Госорганы в сфере ИТ и защиты информации

В России это Росстандарт, ФСТЭК (для средств защиты и аттестации ИС), ФСБ (для криптографии) и Росаккредитация (надзор за органами по сертификации) .

---

11. Что понимается под сертификацией ИС и её цели

Сертификация ИС — это подтверждение соответствия информационной системы требованиям безопасности, стандартам и условиям договоров. Главные цели — обеспечить информационную безопасность, конфиденциальность, целостность и бесперебойность работы системы, а также соответствие нормативно-правовой базе .

12. Направления проверки ИС

В процессе проверки анализируются:

- Архитектура и состав компонентов системы.
- Требования к конфигурации серверного и сетевого оборудования.
- Политики безопасности и управление доступом.
- Защита данных (шифрование, резервное копирование).
- Обучение персонала и организационные меры .

13. Классы стандартов и Common Criteria (ISO/IEC 15408)

Для оценки безопасности ИТ применяются международные и национальные стандарты. **Common Criteria (ISO/IEC 15408)** — это международный стандарт, определяющий унифицированную структуру для оценки безопасности информационных технологий. Он позволяет сравнивать уровень защищенности различных продуктов .

14. Уровень доверия к безопасности (EAL)

EAL (Evaluation Assurance Level) — это оценка строгости проверки безопасности продукта, от 1 до 7. Более высокий уровень означает, что продукт подвергался более глубокому анализу и испытаниям, что подтверждает его повышенную надежность .

15. Российские нормативные акты для ИС

Основные документы: Федеральный закон № 149-ФЗ «Об информации...», Федеральный закон № 152-ФЗ «О персональных данных», а также приказы ФСТЭК России (например, № 17 и № 21), устанавливающие требования к защите информации в государственных ИС и системах персональных данных .

Все ответы могут быть сформулированы в другой близкой по смыслу формулировке