МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»

Смоленский казачий институт промышленных технологий и бизнеса (филиал)

УТВЕРЖДАЮ
Председатель ПЦК
_____Максаков С. А.
«10» апреля 2026 г.

Рабочая программа дисциплины
ОП.07 Технические средства информатизации

Закреплена за **ПЦК общепрофессиональных дисциплин; профессиональных модулей специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Специальность: **10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Направленность

на базе основного общего образования

Квалификация **техник по защите информации**

Форма обучения **очная**

Общая трудоемкость **98 часов**

Часов по учебному плану 98

в том числе:

контактная работа 80

самостоятельная работа 10

часов на контроль 6

Виды контроля в семестрах:

Экзамен - 3

Распределение часов дисциплины по семестрам

Вид учебной работы	Трудоемкость, часов			
	семестр 3		Итого	
	УП	РП	УП	РП
Лекции	48	48	48	48
Практические	32	32	32	32
Контактная работа	80	80	80	80
Сам. работа	10	10	10	10
Часы на контроль	6	6	6	6

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00F5 665F CCDB 5046 05DD 6E08 EBCB D00A DC
Действителен: с 21 октября 2025 г. по 14 января 2027 г.
Владелец: Коржикова Надежда Сергеевна
Должность: Директор

Москва, 2026

Программу составил:
Преподаватель Максаков Сергей Анатольевич _____

Рабочая программа дисциплины
Технические средства информатизации

Разработана в соответствии с:
Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 09.12.2016 г. № 1553)
06.033. Профессиональный стандарт "СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ", утверждённый приказом Министерства труда и социальной защиты Российско Федерации от 14 сентября 2022 г. N 525н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный N 70543)

Разработана на основании учебного плана, утвержденного Учёным советом ФГБОУ ВО "МГУТУ им. К.Г. Разумовского (ПКУ)" от 26.03.2026 протокол №9.

СОДЕРЖАНИЕ

1. МЕСТО ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (УЧЕБНОГО ПРЕДМЕТА)

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	ОП

Дисциплина Технические средства информатизации является частью неопознанный объект и обязательна для изучения.

Требования к предварительной подготовке обучающегося:	
1	Дополнительные учебные предметы, курсы по выбору
2	Индивидуальный проект (Информатика)
3	Математика
4	Основы профессиональной деятельности
5	Профильные учебные предметы
6	Физика
Дисциплины (модули) и практики, для которых освоение данной дисциплины необходимо как предшествующее:	
1	Организационно-правовое обеспечение информационной безопасности
2	Сети и системы передачи информации
3	Электроника и схемотехника
4	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
5	Программные и программно-аппаратные средства защиты информации
6	Учебная практика (защита информации в автоматизированных системах программными и программно-аппаратными средствами)
7	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
8	Производственная практика (защита информации в автоматизированных системах программными и программно-аппаратными средствами)
9	Экзамен по модулю (защита информации в автоматизированных системах программными и программно-аппаратными средствами)
10	Экономика и управление
11	Эксплуатация компьютерных сетей
12	Производственная практика (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)
13	Учебная практика (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)
14	Экзамен по модулю (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

Цели освоения: Формирование у обучающихся системы теоретических знаний и практических навыков в области технического обеспечения автоматизированных (информационных) систем в защищенном исполнении, включая вопросы эксплуатации, технического обслуживания, диагностики неисправностей и настройки программно-аппаратных средств защиты информации.

Задачи: 1. Изучить состав, структуру и принципы функционирования технических средств автоматизированных информационных систем, используемых в защищенном исполнении.

2. Сформировать умения по проверке технического состояния, проведению регламентных работ и текущего ремонта оборудования информационных систем.

3. Освоить методы выявления, локализации и устранения отказов и восстановления работоспособности технических средств.

4. Приобрести навыки установки, настройки и сопровождения программно-аппаратных средств защиты информации.

5. Развить способность выбирать рациональные способы решения профессиональных задач в различных контекстах эксплуатации информационных систем.

Изучение дисциплины направлено на формирование у обучающихся следующих компетенций:

ОК 01.: Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 01.1: Знать актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структуру плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте; методы работы в профессиональной и смежных сферах; порядок оценки результатов решения задач профессиональной деятельности
ОК 01.2: Уметь 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 или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)

ПК 1.4.: Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
ПК 1.4.1: Знать принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации
ПК 1.4.2: Уметь обеспечивать работоспособность, обнаруживать и устранять неисправности
ПК 1.4.3: Иметь практический опыт диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
ПК 2.1.: Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.1.1: Знать особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
ПК 2.1.2: Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
ПК 2.1.3: Иметь практический опыт установки, настройки программных средств защиты информации в автоматизированной системе

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов, тем и содержание занятий /вид занятия/	Семестр / Курс	Часов/ в том числе	Компетен-ции	Виды контроля
	1. РАЗДЕЛ 1. ОСНОВЫ ПОСТРОЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ИНФОРМАТИЗАЦИИ				
1. 1	Тема 1.1. Классификация и общая характеристика технических средств информатизации. Роль технических средств в автоматизированных системах. Классификация технических средств по функциональному назначению (средства сбора, передачи, обработки, хранения, отображения информации). Основные технические характеристики и параметры. Требования к техническим средствам в защищенном исполнении. Знать: определение технических средств информатизации; основные классы технических средств; принципы классификации; номенклатуру основных характеристик; особенности требований для защищенных систем. /Лек/	3	2/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
1. 2	Практическая работа № 1. Изучение состава и характеристик технических средств рабочей станции Уметь: идентифицировать основные компоненты компьютера; определять их технические параметры по маркировке и документации; составлять спецификацию оборудования. Владеть: навыками работы с системными утилитами для определения конфигурации оборудования; навыками чтения технической документации. /Пр/	3	2/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе
1. 3	Тема 1.2. Элементная база и архитектура вычислительных средств. Физические основы работы электронных компонентов (микропроцессоры, контроллеры, память, интерфейсы). Архитектура персонального компьютера и серверных платформ. Структура системной шины, периферийные устройства. Принципы организации ввода-вывода. Особенности архитектуры для систем с повышенными требованиями безопасности.	3	4/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос

	Знать: состав и назначение основных элементов вычислительной системы; принципы работы процессора, видов памяти, контроллеров; архитектурные особенности защищенных вычислительных комплексов; стандартные интерфейсы подключения оборудования. /Лек/				
1. 4	Практическая работа № 2. Настройка параметров BIOS/UEFI и диагностика загрузки. Уметь: входить в программу настройки BIOS/UEFI; изменять параметры загрузки, управления питанием, порядка опроса устройств; проводить начальную диагностику ошибок загрузки. Владеть: навыками настройки базовых параметров системной платы; навыками интерпретации звуковых и видеосигналов ошибок. /Пр/	3	2/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе
1. 5	Тема 1.3. Средства хранения и резервирования данных. Типы накопителей (HDD, SSD, RAID-массивы, ленточные библиотеки). Физические и логические принципы хранения информации. Организация резервного копирования и обеспечение отказоустойчивости. Средства контроля целостности данных. Особенности применения в защищенных системах. Знать: виды накопителей и их характеристики; принципы работы RAID-массивов разных уровней; способы резервирования; методы контроля целостности данных; требования к носителям в защищенном исполнении. /Лек/	3	6/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
1. 6	Практическая работа № 3. Организация RAID-массива и проверка его работоспособности. Уметь: создавать RAID-массивы уровней 0, 1, 5 на контроллере или средствами ОС; моделировать отказ диска и выполнять восстановление; оценивать производительность. Владеть: навыками настройки RAID-контроллера; навыками восстановления данных после сбоя; навыками мониторинга состояния массива. /Пр/	3	2/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе
1. 7	Самостоятельная работа по разделу на тему "Составление структурной схемы технических средств для типового автоматизированного рабочего места защищенной системы" /СР/	3	2/0	ОК 01.1,ОК 01.2,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3,ПК 2.1.1,ПК 2.1.2,ПК 2.1.3	Вопросы для самоподготовки
	2. РАЗДЕЛ 2. ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И ДИАГНОСТИКА СРЕДСТВ ИНФОРМАТИЗАЦИИ				
2. 1	Тема 2.1. Организация технической эксплуатации автоматизированных систем. Нормативно-техническая документация по эксплуатации. Регламенты технического обслуживания (ежедневное, еженедельное, месячное, годовое). Планово-предупредительные ремонты. Система учета отказов и наработки. Документирование результатов проверок. Особенности эксплуатации в защищенном исполнении (ограничения доступа, специальные	3	4/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос

	режимы). Знать: перечень нормативных документов по эксплуатации ТСИ; виды регламентных работ; периодичность обслуживания; порядок ведения эксплуатационной документации; требования к организации рабочих мест в защищенных системах. /Лек/				
2. 2	Практическая работа № 4. Проведение регламентного технического обслуживания ПК Уметь: выполнять внешний осмотр; проверять крепления, контакты, систему охлаждения; очищать от пыли; проверять напряжения блока питания; составлять акт технического состояния. Владеть: навыками проведения ежедневного и ежемесячного обслуживания; навыками работы с измерительными приборами (мультиметр); навыками оформления документации. /Пр/	3	4/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе
2. 3	Тема 2.2. Диагностика технического состояния оборудования. Методы и средства диагностики (встроенный самоконтроль, внешние тестеры, программные диагностические утилиты). Диагностика блока питания, системной платы, памяти, накопителей, сетевых адаптеров. Оценка температурных режимов и вентиляции. Логические и физические методы проверки. Диагностические коды ошибок. Знать: основные методы диагностики; состав диагностического инструментария; алгоритмы проверки ключевых компонентов; признаки неисправностей; правила безопасности при диагностике. /Лек/	3	4/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
2. 4	Практическая работа № 5. Диагностика неисправностей с использованием программных средств. Уметь: использовать диагностические утилиты; интерпретировать результаты тестов; выявлять ошибки памяти, поверхности диска, перегрев компонентов. Владеть: навыками запуска и настройки диагностического ПО; навыками анализа логов; навыками принятия решения о замене компонента. /Пр/	3	4/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе
2. 5	Тема 2.3. Типовые неисправности и способы их устранения. Классификация отказов (постоянные, перемежающиеся, скрытые). Отказы источников питания, материнских плат, оперативной памяти, накопителей, интерфейсных кабелей. Методика поиска неисправности «от общего к частному». Замена модулей и компонентов. Восстановление работоспособности после сбоев электропитания. Работа с аварийными режимами. Знать: типовые симптомы неисправностей для каждого класса устройств; порядок замены компонентов; алгоритмы локализации отказа; способы временного восстановления; критерии окончательного ремонта. /Лек/	3	6/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
2. 6	Практическая работа № 6. Устранение типовых отказов и восстановление работоспособности. Уметь: производить замену блока питания, планки памяти, жесткого диска, кабелей;	3	4/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК	Отчет по практической работе

	восстанавливать загрузку ОС после аппаратного сбоя; сбрасывать настройки BIOS. Владеть: навыками замены горячего и холодного резерва; навыками восстановления конфигурации; навыками проверки работоспособности после ремонта. /Пр/			2.1.2,ПК 2.1.3	
2. 7	Тема 2.4. Техническое обслуживание систем охлаждения и электропитания. Конструкция и принцип работы блоков питания, ИБП, систем охлаждения. Параметры качества электропитания. Замена вентиляторов, чистка от пыли, контроль температуры. Проверка аккумуляторных батарей ИБП. Меры безопасности при работе с высоковольтными цепями. Знать: устройство блоков питания и ИБП; критерии качества электропитания; порядок технического обслуживания систем охлаждения; периодичность проверки аккумуляторов; правила электробезопасности. /Лек/	3	2/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
2. 8	Тема 2.5. Документирование результатов технического обслуживания и ремонта. Журналы технического состояния, акты проверок, дефектные ведомости. Составление отчетов о восстановлении работоспособности. Порядок оформления заявок на замену оборудования. Электронные системы учета отказов. Требования к документации в защищенных системах. Знать: перечень обязательной эксплуатационной документации; правила заполнения журналов и актов; порядок оформления результатов диагностики; требования к хранению документации. /Лек/	3	2/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Устный опрос
2. 9	Самостоятельная работа по разделу по теме "Разработка алгоритма поиска неисправности для заданного сценария отказа (по выбору преподавателя)". /СР/	3	4/0	ОК 01.1,ОК 01.2,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3,ПК 2.1.1,ПК 2.1.2,ПК 2.1.3	Вопросы для самоподготовки
	3. РАЗДЕЛ 3. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ				
3. 1	Тема 3.1. Классификация средств защиты информации технического уровня. Общая структура системы защиты информации. Аппаратные средства криптографической защиты. Средства идентификации и аутентификации (смарт-карты, токены, биометрия). Средства контроля доступа. Средства экранирования и фильтрации. Сертифицированные средства. Знать: классификацию программно-аппаратных СЗИ; назначение основных классов средств; требования к сертификации; принципы работы криптошлюзов, СКЗИ, межсетевых экранов. /Лек/	3	2/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
3. 2	Тема 3.2. Установка и настройка СЗИ на рабочей станции Подготовка аппаратного обеспечения к установке СЗИ. Установка драйверов защищенных устройств. Настройка параметров безопасности	3	4/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос

	на уровне BIOS (Trusted Platform Module, Secure Boot). Инсталляция программных модулей СЗИ. Настройка политик безопасности. Тестирование работоспособности. Знать: последовательность установки СЗИ; требования к аппаратной платформе; способы проверки корректности установки; основные параметры настройки; порядок документирования установки. /Лек/				
3. 3	Практическая работа № 7. Установка и начальная настройка программно-аппаратного СЗИ. Уметь: выполнять предустановочную проверку оборудования; устанавливать драйверы защищенных устройств; активировать Secure Boot и TPM; настраивать базовые политики контроля доступа. Владеть: навыками инсталляции СЗИ; навыками настройки параметров безопасности в BIOS/UEFI; навыками проверки работоспособности после установки. /Пр/	3	4/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе
3. 4	Тема 3.3. Настройка средств криптографической защиты и электронной подписи. Аппаратные генераторы случайных чисел. Установка и конфигурирование СКЗИ (криптопровайдеры, токены, руткиты). Настройка ЭЦП на рабочих станциях. Проверка сертификатов ключей. Обеспечение совместимости с прикладным ПО. Знать: состав СКЗИ; алгоритмы установки ключевых носителей; порядок настройки криптопровайдеров; способы проверки ЭЦП; правила хранения ключевой информации. /Лек/	3	4/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
3. 5	Практическая работа № 8. Настройка криптографического модуля и формирование ключей ЭЦП. Уметь: инициализировать токен (Рутокен, eToken); устанавливать криптопровайдер; генерировать пару ключей; создавать и проверять электронную подпись для тестового документа. Владеть: навыками работы с криптосредствами; навыками импорта/экспорта сертификатов; навыками проверки подлинности подписи. /Пр/	3	4/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе
3. 6	Тема 3.4. Средства защиты от несанкционированного съема информации по техническим каналам. Побочные электромагнитные излучения и наводки (ПЭМИН). Средства пассивной и активной защиты. Заземление, экранирование, фильтрация питания. Средства акустической защиты. Использование генераторов шума. Проверка эффективности мер защиты. Знать: природу технических каналов утечки; типы средств защиты от ПЭМИН; правила заземления и экранирования; порядок проверки эффективности; нормативные требования для защищенных помещений. /Лек/	3	2/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
3. 7	Практическая работа № 9. Проверка эффективности мер защиты от ПЭМИН. Уметь: использовать индикаторы поля; проводить контроль наличия заземления; проверять качество экранирования кабелей; составлять протокол проверки.	3	2/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе

	Владеть: навыками работы с простейшими средствами индикации полей; навыками визуальной проверки целостности экранирующих оболочек; навыками составления акта проверки. /Пр/				
3. 8	Самостоятельная работа по разделу по теме "Составление инструкции по установке и первичной настройке СЗИ для конкретной операционной системы (Windows / Linux)". /СР/	3	2/0	ОК 01.1,ОК 01.2,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3,ПК 2.1.1,ПК 2.1.2,ПК 2.1.3	Вопросы для самоподготовки
	4. РАЗДЕЛ 4. ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ АС В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ				
4. 1	Тема 4.1. Анализ отказов и восстановление в условиях ограничений защищенной системы. Особенности эксплуатации в режиме ограниченного доступа. Порядок допуска к ремонтным работам. Замена оборудования без нарушения целостности средств защиты. Восстановление после сбоев с сохранением криптоключей. Организация взаимодействия со службой безопасности. Знать: регламент допуска ремонтного персонала; алгоритм замены оборудования в защищенной системе; правила сохранения критичной информации; порядок уведомления о нештатных ситуациях. /Лек/	3	2/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
4. 2	Тема 4.2. Восстановление данных после аппаратных сбоев Методы извлечения данных с поврежденных носителей. Программные и аппаратные средства восстановления. Восстановление файловых систем. Использование специализированных аппаратных комплексов (PC-3000 и др.). Соблюдение конфиденциальности при восстановлении. Знать: причины потери данных; методы восстановления на физическом и логическом уровне; перечень средств восстановления; требования к сохранению конфиденциальности; порядок действий при частичном восстановлении. /Лек/	3	2/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
4. 3	Тема 4.3. Проверка работоспособности системы после восстановления. Критерии восстановления работоспособности. Комплексное тестирование всех подсистем. Проверка функционирования СЗИ. Контроль целостности системных файлов и ключевой информации. Оформление акта ввода в эксплуатацию после ремонта. Знать: критерии полного восстановления; состав проверочных тестов; методы контроля целостности; порядок утверждения акта ввода; ответственность персонала. /Лек/	3	2/0	ОК 01.1,ПК 1.4.1,ПК 2.1.1	Устный опрос
4. 4	Практическая работа № 10. Моделирование отказа и восстановление работоспособности защищенной АС. Уметь: имитировать отказ накопителя или блока питания; выполнять замену с соблюдением регламентов защищенной системы;	3	4/0	ОК 01.2,ПК 1.4.2,ПК 1.4.3,ПК 2.1.2,ПК 2.1.3	Отчет по практической работе

	восстанавливать загрузку и проверять работу СЗИ; оформлять акт восстановления. Владеть: навыками действий в нештатной ситуации; навыками восстановления конфигурации защищенного рабочего места; навыками документирования результатов восстановления. /Пр/				
4. 5	Самостоятельная работа по разделу по теме "Разработка плана действий при отказе системного диска на защищенной рабочей станции с криптографическим ключом" /СР/	3	2/0	ОК 01.1,ОК 01.2,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3,ПК 2.1.1,ПК 2.1.2,ПК 2.1.3	Вопросы для самопроверки
	5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ				
5. 1	Консультация «Разбор ключевых тем и типовых задач экзамена по техническим средствам информатизации». Организационные моменты проведения экзамена: формат экзамена; время проведения; разрешённые материалы, используемые студентом во время проведения экзамена; критерии оценивания. Перечисление основных, наиболее важных, тем на экзамене. Краткий обзор разделов, которые будут на экзамене: основы построения технических средств информатизации; техническая эксплуатация и диагностика средств информатизации; программно-аппаратные средства защиты информации; восстановление работоспособности АС в защищенном исполнении. Разбор типовых задач. Примеры задач с пошаговым решением (аналогичные экзаменационным). Ответы на вопросы студентов (студенты могут уточнить сложные моменты и попросить разобрать конкретные задачи). ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации /Конс/	3	2/0	ОК 01.1,ОК 01.2,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3,ПК 2.1.1,ПК 2.1.2,ПК 2.1.3	Вопросы для самоподготовки
5. 2	Экзамен ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации /Эк/	3	6/0	ОК 01.1,ОК 01.2,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3,ПК 2.1.1,ПК 2.1.2,ПК 2.1.3	Вопросы к экзамену, итоговое тестирование

Список выбранных образовательный технологий:

Название	Описание
Информационные технологии	Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта
Компьютерная технология обучения	Основана на использовании информационных технологий в учебном процессе. Реализация данной технологии осуществляется посредством компьютера и иных мультимедийных средств. Использование компьютерных технологий делает учебный процесс не только современным и познавательным, но интересным для обучающихся
Технология поиска информации (Информационная технология)	Информационная технология неотделима от субъектов образовательной деятельности, она является определяющим фактором технологии работы с информацией, применяемой в образовательной практике
Технология организации самостоятельной работы	Организации самостоятельной работы учащихся на более высоком уровне может способствовать применение технологии проектного и проблемного обучения. Методы самостоятельного приобретения знаний основаны на использовании проблемного обучения

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ

Оценочные средства текущего контроля успеваемости:

ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

РАЗДЕЛ 1. ОСНОВЫ ПОСТРОЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ИНФОРМАТИЗАЦИИ

Тема 1.1. Классификация и общая характеристика технических средств информатизации
1. Что понимается под термином «технические средства информатизации» в контексте автоматизированных систем?
2. По каким основным функциональным признакам классифицируются технические средства информатизации?
3. Какие устройства относятся к средствам сбора информации, а какие – к средствам передачи?
4. Чем отличаются средства хранения информации от средств отображения информации по своим задачам?
5. Какие основные технические характеристики важны для оценки производительности вычислительных средств?
6. Какие требования предъявляются к техническим средствам, используемым в системах защищенного исполнения?
7. Какова роль серверного оборудования в структуре автоматизированной системы?
8. Что входит в понятие «периферийное оборудование» информационной системы?
9. Какие нормативные документы регламентируют номенклатуру технических средств в защищенных системах?
10. Почему при выборе технических средств для защищенной системы важно учитывать сертификацию оборудования?

Тема 1.2. Элементная база и архитектура вычислительных средств
1. Какие основные физические принципы лежат в основе работы микропроцессора?
2. Из каких основных функциональных блоков состоит архитектура современного персонального компьютера?
3. Как организована системная шина и какие устройства к ней подключаются?
4. В чем отличие оперативной памяти от постоянной памяти (ПЗУ) по принципу работы и назначению?
5. Какие типы контроллеров ввода-вывода используются в вычислительных системах?
6. Какие архитектурные особенности характерны для вычислительных платформ защищенных информационных систем?
7. Как осуществляется взаимодействие процессора с периферийными устройствами через прерывания и прямой доступ к памяти?
8. Какие интерфейсы (порты) используются для подключения внешних устройств и каковы их основные различия?
9. Что такое микрокод процессора и как он влияет на выполнение команд?
10. Какие дополнительные аппаратные модули (TPM, доверенная загрузка) реализуются на уровне архитектуры для повышения безопасности?

Тема 1.3. Средства хранения и резервирования данных
1. Какие типы накопителей информации наиболее распространены в современных АС и каковы их ключевые характеристики?
2. В чем принципиальное отличие между HDD и SSD с точки зрения физического принципа хранения данных?
3. Что такое RAID-массив и для каких целей он применяется в информационных системах?
4. Какие уровни RAID обеспечивают отказоустойчивость, а какие – только увеличение производительности?
5. Каким образом происходит восстановление данных при отказе одного диска в RAID 5?
6. Какие методы резервного копирования данных существуют и чем они отличаются по времени восстановления?
7. Что такое контрольная сумма и как она используется для проверки целостности хранимых данных?
8. Какие требования к носителям информации предъявляются в защищенных системах (например, по стойкости к магнитным полям)?
9. Как организовано логическое адресное пространство на жестком диске (структура разделов и файловых систем)?
10. Какие программно-аппаратные средства используются для шифрования данных на уровне накопителя?

Тема 1.4. Средства отображения и документирования информации

1. По какому принципу классифицируются устройства отображения информации (мониторы, проекционные панели)?
2. Как формируется цветное изображение на жидкокристаллическом мониторе (LCD)?
3. В чем отличие матричных принтеров от лазерных с точки зрения технологии печати?
4. Какие интерфейсы подключения мониторов и печатающих устройств обеспечивают максимальную скорость передачи данных?
5. Какие технические каналы утечки информации могут возникать при работе монитора и принтера?
6. Какие меры защиты применяются для предотвращения несанкционированного съема информации с экрана?
7. Что такое «защищенный режим печати» и как он реализуется на МФУ?
8. Какие параметры качества печати (разрешение, цветопередача) критичны для документооборота в защищенных системах?
9. Как осуществляется калибровка монитора для точной цветопередачи и зачем она нужна?
10. Какие требования предъявляются к размещению средств отображения в помещении с ограниченным доступом?

РАЗДЕЛ 2. ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И ДИАГНОСТИКА СРЕДСТВ ИНФОРМАТИЗАЦИИ

Тема 2.1. Организация технической эксплуатации автоматизированных систем
1. Какие виды регламентов технического обслуживания существуют и какова их периодичность?
2. Что входит в состав ежедневного технического обслуживания рабочей станции?
3. Какие документы оформляются при проведении планово-предупредительного ремонта?
4. Как ведется учет наработки оборудования и отказов в эксплуатационном журнале?
5. Какие требования предъявляются к организации рабочих мест в защищенном исполнении?
6. Какова процедура допуска персонала к техническому обслуживанию защищенных систем?
7. Какие нормативные акты регламентируют эксплуатацию технических средств информатизации в РФ?
8. Что такое «назначенный срок службы» оборудования и как он учитывается при эксплуатации?
9. Как проводится замена оборудования по окончании срока эксплуатации без нарушения режима безопасности?
10. Какие меры предосторожности необходимо соблюдать при обслуживании работающего оборудования под напряжением?

Тема 2.2. Диагностика технического состояния оборудования
1. Какие методы диагностики (аппаратные, программные, органолептические) применяются для проверки состояния ПК?
2. Какие встроенные средства самодиагностики (POST, BIST) существуют в современных компьютерах?
3. Как расшифровать звуковые сигналы BIOS при ошибках инициализации оборудования?
4. Какие программные утилиты используются для проверки состояния жесткого диска и оперативной памяти?
5. Как оценить температурный режим компонентов и выявить перегрев системного блока?
6. Какие параметры электропитания необходимо проверить при диагностике блока питания?
7. Что такое «стресс-тестирование» системы и с какой целью оно проводится?
8. Как выявить нестабильность работы оперативной памяти (ошибки ECC, сбои при высоких нагрузках)?
9. Какие признаки указывают на выход из строя материнской платы (конденсаторы, дорожки, чипсет)?
10. Как проверить работоспособность сетевого адаптера без подключения к сети?

Тема 2.3. Типовые неисправности и способы их устранения
1. Какие неисправности относятся к категории постоянных, а какие – к перемежающимся отказам?
2. Как определить, что причиной сбоя является именно блок питания, а не материнская плата?
3. Какие действия необходимо выполнить при обнаружении «синего экрана смерти» (BSOD), вызванного аппаратной проблемой?
4. Как локализовать неисправность, если компьютер не включается (нет реакции на кнопку питания)?
5. Что делать в случае появления «битых» секторов на жестком диске и можно ли их восстановить?
6. Каков алгоритм замены вышедшего из строя модуля оперативной памяти?
7. Как устранить проблему с отсутствием изображения на мониторе при работающем системном блоке?
8. Какие временные решения применяются для восстановления работоспособности при отсутствии запасных деталей?
9. Как определить, что неисправен USB-порт, а не подключаемое устройство?
10. Какие типичные механические повреждения встречаются у разъемов и кабелей и как их устранить?

Тема 2.4. Техническое обслуживание систем охлаждения и электропитания
1. Из каких основных элементов состоит система охлаждения современного ПК и как они взаимодействуют?
2. Какова оптимальная температура работы процессора и видеокарты, и чем опасен ее перегрев?
3. Как правильно проводить чистку системного блока от пыли с использованием сжатого воздуха и антистатики?
4. Как проверить уровень заряда и состояние аккумуляторной батареи в источнике бесперебойного питания (ИБП)?
5. По каким параметрам оценивается качество электропитания (напряжение, пульсации, частота)?
6. Какие меры безопасности необходимо соблюдать при работе с блоком питания, содержащим высоковольтные конденсаторы?
7. Как часто следует заменять термопасту на процессоре и как правильно это делать?
8. Что такое «переходное сопротивление» в электрических соединениях и как оно влияет на питание компонентов?
9. Как настроить ИБП для автоматического выключения сервера при длительном пропадании питания?
10. Какие признаки указывают на скорый выход из строя вентилятора охлаждения?

Тема 2.5. Документирование результатов технического обслуживания и ремонта

1. Какие виды эксплуатационной документации являются обязательными для ведения в организации?
2. Какую информацию обязательно содержит акт проверки технического состояния оборудования?
3. Как составляется дефектная ведомость и на основании каких данных она заполняется?
4. Каков порядок оформления заявки на замену оборудования вышедшего из строя?
5. Как отражается факт восстановления работоспособности в журнале технического обслуживания?
6. Какие требования предъявляются к хранению электронных версий эксплуатационных документов?
7. Какую ответственность несет исполнитель за некорректное оформление документации по ремонту?
8. Как фиксируются результаты диагностики с помощью скриншотов и распечаток логов?
9. Каков порядок утверждения акта ввода оборудования в эксплуатацию после ремонта?
10. Чем отличается документация в защищенных системах от обычной (наличие грифа секретности, особые учетные номера)?

РАЗДЕЛ 3. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тема 3.1. Классификация средств защиты информации технического уровня
1. Что относится к программно-аппаратным средствам защиты информации (СЗИ) и чем они отличаются от программных средств?
2. Какие основные классы аппаратных СЗИ выделяют по функциональному назначению?
3. Какие устройства используются для идентификации и аутентификации пользователей в защищенных системах?
4. В чем отличие смарт-карты от USB-токена с точки зрения способа хранения ключевой информации?
5. Какие средства криптографической защиты относятся к аппаратным (СКЗИ) и какова их роль?
6. Что такое межсетевой экран в аппаратном исполнении и как он защищает локальную сеть?
7. Какие средства экранирования и фильтрации применяются для защиты от электромагнитных наводок?
8. Как осуществляется сертификация аппаратных СЗИ и какие органы ее проводят?
9. Какие биометрические средства аутентификации наиболее часто применяются в АС?
10. Чем отличаются встроенные средства защиты (в процессорах, чипсетах) от внешних модулей?

Тема 3.2. Установка и настройка СЗИ на рабочей станции
1. Какую предварительную проверку оборудования необходимо выполнить перед установкой СЗИ?
2. Как активировать модуль TPM в настройках BIOS/UEFI для поддержки криптографии?
3. Что такое Secure Boot и как он влияет на загрузку защищенной операционной системы?
4. Как устанавливаются драйверы для аппаратных ключей защиты (токенов, ридеров смарт-карт)?
5. Какие параметры политики безопасности необходимо настроить после установки СЗИ?
6. Как проверить, что все компоненты СЗИ установлены корректно и работают без ошибок?
7. В какой последовательности выполняется инсталляция программных модулей СЗИ относительно ОС?
8. Какие конфликты могут возникнуть при установке СЗИ с антивирусным ПО и как их разрешить?
9. Как задокументировать процесс установки СЗИ для последующего воспроизведения?
10. Какие тесты выполняются для подтверждения работоспособности средств защиты после настройки?

Тема 3.3. Настройка средств криптографической защиты и электронной подписи
1. Для чего необходим аппаратный генератор случайных чисел в составе СКЗИ?
2. Как установить криптопровайдер и зарегистрировать его в системе?
3. Каков порядок инициализации токена (например, Рутокен) и генерации ключевой пары?
4. Как создать запрос на сертификат ключа электронной подписи (ЭЦП) и где его получить?
5. Как осуществляется проверка сертификата ключа ЭЦП на действительность (срок, статус)?
6. Как настроить прикладное ПО (например, офисный пакет, СЭД) для работы с ЭЦП?
7. Какие правила хранения ключевых носителей должны соблюдаться в защищенной системе?
8. Как проверить электронную подпись документа и установить ее подлинность?
9. Каковы действия при утере или компрометации ключа ЭЦП?
10. Как настроить автоматическое шифрование данных на диске с использованием аппаратного модуля TPM?

Тема 3.4. Средства защиты от несанкционированного съема информации по техническим каналам
1. Что такое каналы побочных электромагнитных излучений и наводок (ПЭМИН) и почему они опасны?
2. Какие пассивные средства защиты от ПЭМИН применяются (экраны, фильтры, заземление)?
3. Какие активные средства защиты (генераторы шума, маскирующие сигналы) используются в защищенных помещениях?
4. Как правильно организовать заземление оборудования для снижения уровня излучений?
5. Каким образом осуществляется акустическая защита помещений от съема информации через микрофоны?
6. Как проверяется эффективность экранирования кабелей и соединительных линий?
7. Какие приборы применяются для измерения уровня побочных излучений в рабочем помещении?
8. Какие нормативные документы регламентируют требования к защите от ПЭМИН для объектов информатизации?
9. Какую роль играет пространственное размещение оборудования в снижении рисков по техническим каналам?
10. Какие организационные меры (режимные, временные) дополняют аппаратную защиту от ПЭМИН?

РАЗДЕЛ 4. ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ АС В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Тема 4.1. Анализ отказов и восстановление в условиях ограничений защищенной системы
1. Каковы особенности допуска ремонтного персонала к оборудованию защищенной системы?

2. Какие дополнительные риски возникают при замене оборудования в системе с установленными СЗИ?
3. Как сохранить криптографические ключи при замене системного блока или материнской платы?
4. Каков порядок извещения службы безопасности о нештатной ситуации и ремонтных работах?
5. Какие временные ограничения действуют на проведение восстановительных работ в режимных объектах?
6. Как обеспечить сохранность журналов аудита при аварийной остановке системы?
7. Какие меры предосторожности необходимо соблюдать при вскрытии корпуса защищенного оборудования?
8. Как осуществляется координация действий между техническим персоналом и службой защиты информации?
9. Какие последствия могут наступить при нарушении регламента замены оборудования в защищенной системе?
10. Как выполняется замена оборудования, имеющего маркировку «специальное изделие»?

Тема 4.2. Восстановление данных после аппаратных сбоев
1. Какие основные причины приводят к физическому повреждению носителей данных?
2. Какие программные средства восстановления данных применяются при логических повреждениях файловой системы?
3. В чем отличие восстановления данных с HDD от восстановления с SSD с точки зрения технологии?
4. Для каких целей используется аппаратно-программный комплекс PC-3000 и каковы его возможности?
5. Какие действия запрещено выполнять при первых признаках выхода из строя накопителя с ценной информацией?
6. Как осуществляется создание посекторного образа поврежденного диска и для чего это нужно?
7. Какие методы используются для восстановления данных после форматирования или удаления разделов?
8. Как соблюдается конфиденциальность при передаче носителя данных в ремонтную лабораторию?
9. Каков алгоритм действий при частичном восстановлении данных (неполный объем)?
10. Как проверяется целостность восстановленных критически важных файлов (сравнение контрольных сумм)?

Тема 4.3. Проверка работоспособности системы после восстановления
1. Какие критерии позволяют считать систему полностью восстановленной после ремонта?
2. Какие компоненты системы подлежат обязательной проверке после замены оборудования?
3. Как проверить функционирование СЗИ после аппаратного вмешательства в систему?
4. Какие методы контроля целостности системных файлов применяются после восстановления?
5. Как осуществляется проверка сохранности и работоспособности криптографических ключей?
6. Какие тесты производительности (нагрузочные) необходимо провести для подтверждения стабильности работы?
7. Как оформляется акт ввода системы в эксплуатацию после внепланового ремонта?
8. Какие лица подписывают акт восстановления и кто несет ответственность за его результаты?
9. Какой период наблюдения за восстановленной системой считается достаточным для снятия режима «особого контроля»?
10. Какие действия выполняются при обнаружении отклонений в работе после подписания акта восстановления?

ВОПРОСЫ ДЛЯ САМОПОДГОТОВКИ

Самостоятельная работа по разделу на тему "Составление структурной схемы технических средств для типового автоматизированного рабочего места защищенной системы"
1. Какова цель составления структурной схемы автоматизированного рабочего места (АРМ) в защищенном исполнении?
2. Из каких основных аппаратных компонентов состоит типовое защищенное АРМ?
3. Какие средства защиты информации (СЗИ) должны быть отражены на структурной схеме АРМ?
4. Какие периферийные устройства типового АРМ являются критическими с точки зрения информационной безопасности?
5. Чем структурная схема защищенного АРМ отличается от схемы обычного рабочего места?
6. Какие каналы утечки информации должны учитываться при проектировании структурной схемы защищенного АРМ?
7. Какие программные компоненты (операционная система, СЗИ) должны быть включены в структурную схему?
8. Каким образом на структурной схеме отражается взаимодействие АРМ с внешними сетями?
9. Какие требования к аппаратной части АРМ предъявляются при работе с персональными данными?
10. Какие модули доверенной загрузки (например, ViPNet-SafeBoot, «Соболь») могут быть включены в структурную схему защищенного АРМ? -11-12

Самостоятельная работа по разделу по теме "Разработка алгоритма поиска неисправности для заданного сценария отказа (по выбору преподавателя)".
1. Какова цель разработки алгоритма поиска неисправности в защищенной системе?
2. С чего следует начинать процесс диагностики при отказе средств криптографической защиты информации?
3. Какие этапы включает алгоритм поиска неисправности при отказе модуля доверенной загрузки?
4. Каким образом проверяется целостность системных файлов в ходе диагностики неисправности?
5. Какие инструменты используются для проверки работоспособности СЗИ в процессе поиска неисправности?
6. Какова последовательность действий при подозрении на нарушение целостности BIOS/UEFI?
7. Какие признаки указывают на успешное завершение поиска и устранения неисправности?
8. Какие каналы взаимодействия с системным администратором предусмотрены в алгоритме поиска неисправности?
9. Какие действия в алгоритме предусмотрены при выявлении попытки несанкционированного доступа?
10. Каким образом в алгоритме учитывается сохранность данных при устранении неисправности?

Самостоятельная работа по разделу по теме "Составление инструкции по установке и первичной настройке СЗИ для конкретной операционной системы (Windows / Linux)".

1. Какова структура инструкции по установке СЗИ для операционной системы (Windows/Linux)?
2. Какие подготовительные шаги необходимо выполнить перед установкой СЗИ на рабочую станцию?
3. Какие требования к аппаратному обеспечению должны быть проверены перед установкой СЗИ?
4. Каким образом в инструкции описывается процесс установки сертифицированного СЗИ?
5. Какие настройки политик безопасности должны быть заданы после установки СЗИ? -14
6. Как в инструкции описывается процедура проверки корректности установки СЗИ?
7. Какие действия должны быть выполнены для интеграции СЗИ с существующей инфраструктурой безопасности?
8. Какие шаги по настройке контроля устройств (USB, внешние носители) включаются в инструкцию? -15
9. Каким образом в инструкции описывается конфигурирование аудита событий безопасности?
10. Какие меры предосторожности необходимо указать в инструкции при настройке СЗИ?

Самостоятельная работа по разделу по теме "Разработка плана действий при отказе системного диска на защищенной рабочей станции с криптографическим ключом"
1. Какова цель разработки плана действий при отказе системного диска на защищенной АРМ?
2. Какие первоочередные действия должны быть предприняты при обнаружении отказа системного диска?
3. Как в плане действий описывается процедура обеспечения сохранности криптографического ключа?
4. Каким образом восстанавливается доступ к зашифрованным данным при отказе системного диска?
5. Какие резервные источники криптографических ключей должны быть предусмотрены в плане?
6. Какая последовательность действий требуется для восстановления работоспособности АРМ на новом диске?
7. Как в плане описана процедура проверки работоспособности криптографической защиты после восстановления?
8. Какие действия по уведомлению администратора безопасности предусмотрены в плане?
9. Какие меры по расследованию причин отказа системного диска включены в план действий?
10. Каким образом план действий учитывает требования нормативных документов по защите информации?

ЗАДАНИЯ ДЛЯ ПРАКТИЧЕСКИХ РАБОТ

РАЗДЕЛ 1. ОСНОВЫ ПОСТРОЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ИНФОРМАТИЗАЦИИ

Практическая работа № 1. Изучение состава и характеристик технических средств рабочей станции
Задания:
1. Определите по внешнему виду и маркировке системного блока тип процессора, объем оперативной памяти и модель материнской платы. Результаты зафиксируйте в виде перечня компонентов.
2. Используя системную утилиту (например, «Сведения о системе» или Device Manager), составьте полный перечень установленного оборудования с указанием производителей и версий драйверов.
3. По маркировке блока питания определите его мощность, количество линий питания и тип разъемов. Сравните с потребляемой мощностью установленных компонентов и сделайте вывод о достаточности блока питания.
4. Идентифицируйте все интерфейсные порты на задней панели системного блока (USB, HDMI, DisplayPort, RJ-45, аудиоразъемы). Определите их версии и пропускную способность по документации к материнской плате.
5. По серийным номерам и моделям накопителей (HDD/SSD) определите их объем, скорость вращения шпинделя (для HDD) и тип интерфейса. Сравните фактические характеристики с заявленными в документации производителя.
6. Проведите визуальный осмотр системной платы и определите расположение основных чипов (чипсет, контроллеры ввода-вывода, звуковой кодек, сетевой контроллер). Зафиксируйте их обозначения.
7. Составьте спецификацию оборудования рабочей станции в виде сводной ведомости, включив в нее все выявленные компоненты с их краткими характеристиками.
8. По маркировке планок оперативной памяти определите тип памяти (DDR3/DDR4/DDR5), тактовую частоту и тайминги. Проверьте, работают ли планки в двухканальном режиме.
9. Определите наличие и тип дополнительных контроллеров (например, SATA-контроллер, RAID-контроллер, контроллер USB 3.0). Укажите их функциональное назначение.
10. На основе собранных данных заполните паспорт технического средства (формуляр) по установленной в организации форме, указав все идентификационные номера и основные параметры.

Практическая работа № 2. Настройка параметров BIOS/UEFI и диагностика загрузки
Задания:
1. Выполните вход в программу настройки BIOS/UEFI (определите необходимую клавишу при старте). Зафиксируйте текущую версию прошивки и дату ее выпуска.
2. Настройте порядок загрузки устройств (Boot Order) так, чтобы первым загружался загрузочный USB-накопитель, вторым – системный диск, третьим – сетевой загрузчик. Сохраните изменения и проверьте правильность порядка после перезагрузки.
3. Настройте параметры управления питанием (Power Management), установив режим энергосбережения и отключив функцию автоматического включения при подаче питания.
4. Включите поддержку виртуализации (Intel VT-x / AMD-V) и настройте параметры безопасности, касающиеся защиты от выполнения вредоносного кода.
5. Выполните сброс настроек BIOS/UEFI на параметры «по умолчанию» (Load Defaults), а затем заново задайте только порядок загрузки и дату/время.
6. Пронаблюдайте процедуру POST (самодиагностика при включении) и запишите все звуковые сигналы и текстовые сообщения на экране. Определите по ним, успешно ли прошла инициализация всех устройств.
7. Намеренно измените один из критических параметров (например, тип работы SATA-контроллера с AHCI на IDE) и проанализируйте, возникла ли ошибка загрузки. Верните параметр в исходное состояние и зафиксируйте результат.

8. Настройте параметры безопасности: установите пароль администратора BIOS и пароль на загрузку системы. Проверьте их действие при входе в настройки и при старте ПК.
9. Включите функцию быстрой загрузки (Fast Boot) и отключите отображение логотипа производителя при старте. Оцените изменение времени загрузки системы.
10. Сохраните текущую конфигурацию BIOS/UEFI в виде профиля (если поддерживается) или запишите все измененные параметры в отчет для возможного восстановления настроек.

Практическая работа № 3. Организация RAID-массива и проверка его работоспособности
Задания:
1. Определите наличие встроенного RAID-контроллера на материнской плате и его поддерживаемые уровни RAID (0, 1, 5, 10) по документации или при входе в утилиту настройки RAID.
2. Используя два или три доступных физических диска одинакового объема, создайте RAID-массив уровня 1 (зеркало) и выполните его инициализацию.
3. На созданном RAID-массиве создайте один логический том и выполните его форматирование в файловую систему NTFS. После этого скопируйте на него тестовый набор файлов.
4. Сымитируйте отказ одного из дисков в массиве RAID 1 (извлеките его или переведите в состояние «Offline»). Определите, сохранилась ли работоспособность системы и доступность данных.
5. Выполните процедуру добавления нового диска вместо отказавшего и запустите процесс ребилда (восстановления зеркала). Понаблюдайте за индикацией прогресса восстановления.
6. Создайте RAID-массив уровня 0 (чередование) из двух дисков и измерьте скорость чтения/записи с помощью простого копирования крупного файла. Сравните результат со скоростью одиночного диска.
7. Для RAID-массива уровня 5 (из трех дисков) рассчитайте общий полезный объем и укажите, какой объем используется для хранения контрольных сумм.
8. Проверьте утилитой управления RAID (например, Intel RST или AMD RAIDXpert) состояние всех дисков: температуру, количество ошибок чтения/записи, время наработки.
9. Выполните тест на отказ диска в RAID 5 и произведите его замену. Зафиксируйте время восстановления и состояние массива после завершения ребилда.
10. Сравните надежность и производительность трех уровней RAID (0, 1, 5) на основе выполненных экспериментов и сформулируйте рекомендации по применению каждого уровня для разных задач (база данных, файловый сервер, система хранения резервных копий).

РАЗДЕЛ 2. ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И ДИАГНОСТИКА СРЕДСТВ ИНФОРМАТИЗАЦИИ

Практическая работа № 4. Проведение регламентного технического обслуживания ПК
Задания:
1. Проведите внешний осмотр системного блока, монитора и периферийных устройств. Проверьте целостность корпусов, состояние кабелей и разъемов. Отметьте обнаруженные механические повреждения.
2. Выполните очистку системного блока от пыли внутри с использованием баллона со сжатым воздухом и кисти. Особое внимание уделите радиаторам процессора, видеокарты и блоку питания.
3. Проверьте надежность крепления всех внутренних компонентов: плат расширения, планок памяти, кабельных соединений. Подтяните все винтовые соединения и защелки.
4. Выполните проверку работы системы охлаждения: определите обороты всех вентиляторов через BIOS или утилиту мониторинга, убедитесь в отсутствии посторонних шумов.
5. Проведите диагностику блока питания с помощью мультиметра – измерьте напряжения на разъемах питания (3,3 В, 5 В, 12 В) при работе системы под нагрузкой и в простое. Занесите показания в протокол.
6. Выполните тестирование монитора на битые пиксели и равномерность подсветки с использованием тестовых утилит или онлайн-сервисов. Результаты зафиксируйте.
7. Проверьте состояние интерфейсных кабелей (USB, HDMI, сетевых патч-кордов) на предмет перегибов, обрывов и надежности контактов. Замените при необходимости.
8. Проверьте уровень шума и вибрации системного блока. При обнаружении избыточной вибрации определите источник (диски, вентиляторы) и примите меры (замена, демпфирование).
9. Проведите проверку подключения заземления корпуса системного блока и экранов кабелей. При отсутствии заземления – организуйте его временно или зафиксируйте нарушение в акте.
10. Составьте акт технического состояния оборудования после проведенного обслуживания, указав в нем все выполненные операции, выявленные дефекты и рекомендации по дальнейшей эксплуатации.

Практическая работа № 5. Диагностика неисправностей с использованием программных средств
Задания:
1. Используя диагностическую утилиту AIDA64 (или аналоги), получите полный отчет об аппаратной конфигурации системы и сохраните его в текстовом файле.
2. Выполните тест оперативной памяти с помощью утилиты MemTest86+ (или Windows Memory Diagnostic). Запустите полный цикл тестов и проанализируйте отчет об ошибках.
3. Проверьте состояние жесткого диска (HDD) с помощью программы Victoria или HD Tune: определите наличие битых секторов, время доступа и состояние SMART-атрибутов.
4. Для SSD-накопителя выполните проверку с помощью утилиты производителя (например, Samsung Magician или Intel SSD Toolbox), оценив общий объем записанных данных и оставшийся ресурс (TBW).
5. С помощью утилиты мониторинга температуры (HWMonitor или Open Hardware Monitor) зафиксируйте температуры процессора, видеокарты, чипсета и накопителей в состоянии простоя и под стрессовой нагрузкой.

6. Запустите стресс-тест процессора и оперативной памяти с помощью утилиты Prime95 или OCCT в течение 15 минут. Отслеживайте появление ошибок вычислений или перегрев.
7. Проведите диагностику сетевого адаптера с помощью команд ping и tracert, отправляя запросы к локальному шлюзу и внешнему серверу. Проанализируйте потери пакетов и время задержки.
8. Проверьте целостность системных файлов операционной системы с помощью утилиты SFC /SCANNOW. Зафиксируйте, были ли найдены поврежденные файлы и выполнено ли их восстановление.
9. С помощью программы CrystalDiskInfo оцените общее состояние всех накопителей по показателям SMART. Сделайте прогноз вероятного выхода из строя для каждого диска.
10. На основе всех выполненных тестов составьте итоговое заключение о техническом состоянии оборудования с указанием критических замечаний (дефектов) и рекомендуемых действий.

Практическая работа № 6. Устранение типовых отказов и восстановление работоспособности
Задания:
1. Сымитируйте отказ блока питания (отключите его от материнской платы). Выполните проверку мультиметром и определите, какой из выходных напряжений отсутствует. Произведите замену на заведомо исправный блок питания и убедитесь в загрузке системы.
2. Замените одну планку оперативной памяти на заведомо неисправную (или извлеките ее). Проанализируйте поведение системы (звуковые сигналы, отсутствие изображения). Установите исправную планку на ее место и проверьте восстановление.
3. Выполните замену вышедшего из строя жесткого диска. Установите новый диск, создайте разделы и восстановите загрузочную запись, используя установочный диск операционной системы.
4. Сбросьте настройки BIOS/UEFI на заводские при помощи перемычки Clear CMOS на материнской плате (или извлечения батарейки). После этого заново сконфигурируйте параметры загрузки и дату.
5. При возникновении ошибки «Boot device not found» определите причину (отключенный диск, нарушенный порядок загрузки, поврежденный загрузчик). Восстановите загрузку с помощью загрузочного диска и команд bootrec /fixmbr, /fixboot.
6. Замените поврежденный SATA-кабель и убедитесь, что система стала стабильно определять накопитель. Проверьте скорость передачи данных после замены кабеля.
7. При появлении сообщения о перегреве процессора (CPU overheat) проверьте контакт радиатора, замените термопасту и закрепите крепление. Запустите мониторинг температур и убедитесь в нормализации.
8. Выполните замену кнопки включения на корпусе (или замыкание контактов на плате) при отказе кнопки. Обучитесь аварийному запуску системы без корпусной кнопки.
9. Восстановите работоспособность операционной системы после сбоя, используя загрузку в безопасном режиме и откат к последней удачной конфигурации.
10. После каждого ремонтного действия проверяйте работоспособность системы в полном объеме (загрузка ОС, запуск тестовых приложений, сетевая доступность) и фиксируйте результат в журнале ремонта.

РАЗДЕЛ 3. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Практическая работа № 7. Установка и начальная настройка программно-аппаратного СЗИ
Задания:
1. Проверьте соответствие аппаратной платформы требованиям выбранного СЗИ (процессор, объем ОЗУ, наличие TPM-модуля, свободное место на диске). Составьте заключение о готовности.
2. Выполните активацию модуля TPM и включение технологии Secure Boot в настройках UEFI. Проверьте, что система загружается с включенными параметрами безопасности.
3. Установите дистрибутив программно-аппаратного СЗИ (например, средства криптографической защиты или систему доверенной загрузки) согласно инструкции производителя.
4. Установите драйверы для USB-токена (или смарт-карт ридера) и проверьте, что устройство корректно определилось в системе и отображается в диспетчере устройств.
5. Настройте базовые политики контроля доступа в СЗИ: задайте минимальную длину пароля, количество попыток входа, время блокировки сеанса при неактивности.
6. После установки выполните регистрацию администратора СЗИ, создайте учетную запись с административными правами и установите первичные ключи доступа.
7. Проведите тестирование установленного СЗИ: попробуйте запустить разрешенные и запрещенные приложения, попытайтесь отключить службы защиты (с проверкой реакции системы).
8. Создайте резервную копию всех настроек СЗИ на защищенный носитель и сохраните ее в соответствии с требованиями организации.
9. Задокументируйте процесс установки и начальной настройки в виде протокола с указанием версий ПО, серийных номеров аппаратных модулей и установленных параметров.
10. Выполните проверку целостности установленных файлов СЗИ с использованием встроенных средств самоконтроля и зафиксируйте результаты.

Практическая работа № 8. Настройка криптографического модуля и формирование ключей ЭЦП
Задания:
1. Инициализируйте USB-токен (например, Рутокен или eToken): установите PIN-код администратора и пользователя, выполните разметку памяти устройства.
2. Установите криптопровайдер, совместимый с вашим токеном (например, КриптоПро CSP). Проверьте корректность установки через тестовый вызов провайдера.

3. Сгенерируйте пару ключей (закрытый и открытый) для электронной подписи на токене, указав необходимые алгоритмы и длину ключа согласно требованиям.
4. Сформируйте запрос на сертификат ключа подписи (PKCS#10) и сохраните его в файл. В запросе укажите все необходимые данные владельца (ФИО, должность, организацию).
5. Получив от преподавателя тестовый корневой сертификат, подпишите свой запрос и импортируйте полученный сертификат в хранилище сертификатов Windows или в токен.
6. Создайте тестовый текстовый документ (например, в MS Word) и сформируйте для него электронную подпись, используя установленный СКЗИ и закрытый ключ из токена.
7. Выполните проверку подписи созданного документа: убедитесь, что подпись действительна, срок действия сертификата не истек, а подпись соответствует содержимому документа.
8. Экспортируйте открытый сертификат в файл формата .cer и отправьте его другому студенту для проверки возможности верификации подписанного документа.
9. Проверьте подлинность документа, подписанного вашим соседом, используя его открытый сертификат. Сделайте скриншот результата верификации.
10. Настройте программное обеспечение (например, офисный пакет или СЭД) на автоматическое использование вашего сертификата при создании подписи по умолчанию. Проверьте корректность работы в тестовом режиме.

Практическая работа № 9. Проверка эффективности мер защиты от ПЭМИН
Задания:
1. Проведите визуальный осмотр помещения информатизации на предмет наличия экранирующих покрытий на стенах, окнах и дверях. Занесите наблюдения в протокол.
2. Проверьте наличие заземления у всех подключенных технических средств (компьютеров, серверов, ИБП). Отметьте устройства без заземления.
3. При помощи мультиметра измерьте сопротивление между заземляющей шиной и корпусами системных блоков. Проверьте, не превышает ли оно допустимых нормативов.
4. Осмотрите все сетевые и интерфейсные кабели (USB, HDMI, VGA, Ethernet) на наличие ферритовых фильтров и экранирующих оплеток. Определите, где защита отсутствует.
5. С помощью портативного индикатора поля (или простого радиоприемника) оцените уровень электромагнитных излучений в ближней зоне от системного блока и монитора.
6. Проверьте, защищены ли окна помещения металлической сеткой или специальной пленкой для снижения уровня излучения наружу. Зафиксируйте результат.
7. Проверьте корректность подключения сетевого фильтра (источника бесперебойного питания) с функцией фильтрации высокочастотных помех и наличие подавления импульсных перенапряжений.
8. Сравните уровень наводок при работе ПК с открытым и закрытым металлическим корпусом (крышкой). Сделайте вывод об эффективности корпуса как экрана.
9. Составьте схему расположения оборудования в помещении с указанием расстояний между рабочими станциями, серверами и экранирующими элементами.
10. На основе всех проверок оформите акт проверки эффективности мер защиты от ПЭМИН, перечислив выявленные недостатки и дав рекомендации по их устранению.

РАЗДЕЛ 4. ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ АС В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Практическая работа № 10. Моделирование отказа и восстановление работоспособности защищенной АС
Задания:
1. В учебном стенде, представляющем защищенную автоматизированную систему, зафиксируйте исходное состояние: состав оборудования, установленные СЗИ, наличие резервных копий ключей и данных.
2. Сымитируйте отказ системного накопителя (отключите питание SATA-диска), на котором хранится операционная система и криптографические ключи.
3. Выполните диагностику и подтвердите факт отказа накопителя. Оформите в журнале запись о неисправности с указанием времени, симптомов и предполагаемой причины.
4. С соблюдением регламента защищенной системы (запрос разрешения, оповещение службы безопасности) произведите замену отказавшего накопителя на новый.
5. Восстановите систему с резервного образа (или выполните чистую установку ОС с последующим восстановлением конфигурации СЗИ из резервной копии).
6. Импортируйте ранее сохраненные криптографические ключи и сертификаты на новый носитель (или восстановите из резервной копии на токен).
7. Проверьте функционирование всех установленных средств защиты (контроль доступа, шифрование, электронная подпись) после восстановления.
8. Выполните комплексное тестирование всей системы: загрузка ОС, запуск прикладного ПО, сетевое взаимодействие, работа с защищенными документами.
9. Оформите акт восстановления работоспособности защищенной АС с указанием причин отказа, выполненных действий, результатов проверок и подписей ответственных лиц.
10. Внесите запись о проведенном восстановлении в электронный и бумажный журнал учета отказов, указав время простоя системы и рекомендуемые профилактические меры для предотвращения повторного отказа.

Оценочные средства промежуточной аттестации:

ВОПРОСЫ К ЭКЗАМЕНУ

Индикатор ЗНАТЬ

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
1. Установите правильную последовательность действий при проведении планового технического обслуживания персонального компьютера.
А) Очистка внутренних компонентов от пыли
Б) Внешний осмотр корпуса и кабелей
В) Проверка работоспособности системы после обслуживания
Г) Проверка надежности крепления компонентов и затяжка винтов
2. Установите правильную последовательность действий при диагностике неисправности компьютера, который не включается.
А) Проверка наличия напряжения в розетке и подключения кабеля питания
Б) Замена блока питания на заведомо исправный
В) Проверка состояния кнопки включения на корпусе
Г) Проверка работоспособности материнской платы (визуальный осмотр, тестовый запуск)
3. Установите соответствие между типом неисправности и ее характерным внешним признаком.
А) Неисправность блока питания
Б) Неисправность оперативной памяти
В) Перегрев процессора
Г) Повреждение загрузочного сектора диска
1. Компьютер включается, но при запуске ОС появляется ошибка "Boot device not found"
2. Компьютер внезапно перезагружается или выключается во время работы под нагрузкой
3. При включении компьютера раздаются повторяющиеся длинные звуковые сигналы, изображения нет
4. Компьютер не реагирует на нажатие кнопки включения, вентиляторы не вращаются
5. Система работает медленно, часто зависает, при просмотре видео появляются артефакты
4. Установите соответствие между устройством компьютера и его основным назначением.
А) Блок питания
Б) Системная плата
В) Оперативная память
Г) Видеокарта
1. Хранение временных данных и исполняемого кода для быстрого доступа процессора
2. Преобразование сигналов для формирования изображения на мониторе
3. Обеспечение электрической связью всех компонентов и их питание через разъемы
4. Преобразование переменного тока сети в постоянные напряжения для питания компонентов
5. Постоянное хранение данных при выключенном питании
5. Установите соответствие между уровнем RAID и его ключевой характеристикой.
А) RAID 0
Б) RAID 1
В) RAID 5
Г) RAID 10
1. Объединение зеркалирования и чередования, высокая отказоустойчивость
2. Данные распределяются по дискам без избыточности, повышается скорость
3. Полное зеркальное копирование данных на два диска
4. Чередование с распределенной четностью, выдерживает отказ одного диска
5. Используется только для архивирования, без повышения производительности

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
6. Установите правильную последовательность действий при создании RAID-массива уровня 1 на встроенном контроллере.
А) Инициализация созданного массива и форматирование логического тома
Б) Выбор дисков для включения в массив и выбор уровня RAID 1
В) Загрузка в утилиту настройки RAID-контроллера
Г) Копирование тестовых файлов на массив и проверка зеркалирования
7. Установите правильную последовательность действий при установке программно-аппаратного средства защиты информации (СЗИ) на рабочую станцию.
А) Активация аппаратных модулей (TPM, Secure Boot) в BIOS/UEFI
Б) Установка драйверов для аппаратных ключей (токенов, смарт-карт)
В) Проверка соответствия аппаратной платформы требованиям СЗИ
Г) Настройка политик безопасности и тестирование работоспособности СЗИ
8. Установите соответствие между средством защиты информации и его функцией.
А) Межсетевой экран (брандмауэр)
Б) Аппаратный токен
В) Система доверенной загрузки
Г) Аппаратный генератор случайных чисел
1. Контроль целостности загружаемой операционной системы и драйверов
2. Фильтрация сетевого трафика по правилам доступа между сетями

3. Хранение закрытых ключей и выполнение криптографических операций
4. Создание непредсказуемых последовательностей для криптографических ключей
5. Резервное копирование критически важной информации
9. Установите соответствие между этапом технического обслуживания и выполняемым действием.
А) Ежедневное обслуживание
Б) Ежемесячное обслуживание
В) Полугодовое обслуживание
Г) Годовое обслуживание
1. Замена термопасты на процессоре и проверка состояния всех конденсаторов
2. Внешний осмотр, проверка подключения кабелей и запуск диагностических утилит
3. Полная очистка системного блока от пыли с разборкой и проверка вентиляторов
4. Проверка журналов событий и резервное копирование критических данных
5. Обновление прошивки BIOS/UEFI и всех драйверов устройств

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
10. Установите правильную последовательность действий при восстановлении работоспособности системы после отказа накопителя в защищенной системе.
А) Замена отказавшего накопителя на новый
Б) Восстановление операционной системы из резервной копии
В) Проверка функционирования средств защиты информации (СЗИ)
Г) Импорт криптографических ключей и сертификатов из резервной копии
11. Установите правильную последовательность этапов проверки эффективности мер защиты от побочных электромагнитных излучений (ПЭМИН) в помещении.
А) Осмотр наличия экранирующих покрытий на стенах и окнах
Б) Проверка наличия заземления у всех технических средств
В) Измерение уровня излучений с помощью индикатора поля
Г) Осмотр кабелей на наличие ферритовых фильтров и экранов
12. Установите правильную последовательность действий при создании и проверке электронной цифровой подписи (ЭЦП) с использованием аппаратного токена.
А) Генерация пары ключей (закрытый и открытый) на токене
Б) Формирование запроса на сертификат и получение сертификата
В) Создание тестового документа и формирование электронной подписи
Г) Проверка подписи документа с использованием открытого сертификата
13. Установите соответствие между диагностической утилитой и ее основным назначением.
А) MemTest86+
Б) CrystalDiskInfo
В) HWMonitor
Г) Victoria
1. Проверка поверхности жесткого диска и поиск битых секторов
2. Тестирование оперативной памяти на наличие ошибок
3. Мониторинг температуры, напряжений и оборотов вентиляторов
4. Оценка состояния накопителей по показателям SMART и прогнозирование отказа
5. Создание загрузочных USB-накопителей
14. Установите соответствие между действием при восстановлении системы и его целью.
А) Восстановление из резервной копии
Б) Замена оборудования на совместимое
В) Проверка целостности системных файлов
Г) Тестирование под нагрузкой
1. Обеспечение физической работоспособности аппаратной части
2. Возврат данных и настроек к состоянию на момент создания копии
3. Выявление скрытых дефектов, проявляющихся при высокой нагрузке
4. Обнаружение поврежденных или отсутствующих файлов операционной системы
5. Установка новых версий драйверов для улучшения совместимости
15. Установите соответствие между техническим средством информатизации и видом выполняемых им операций.
А) Сканер
Б) Принтер
В) Монитор
Г) Микрофон
1. Преобразование электрических сигналов в акустические для записи звука
2. Оптическое считывание информации с бумажного носителя в цифровой формат
3. Преобразование цифрового сигнала в видимое изображение на экране
4. Вывод информации на бумажный носитель с использованием различных технологий печати
5. Передача данных между компьютерами по радиоканалу

Индикатор УМЕТЬ

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

1. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Какое техническое средство в первую очередь необходимо заменить при обнаружении многократных ошибок чтения/записи и появления сбойных секторов по данным SMART-диагностики?
А) Блок питания
Б) Оперативная память
В) Жесткий диск
Г) Материнская плата
2. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При включении компьютера слышны повторяющиеся короткие звуковые сигналы, изображение на мониторе отсутствует. Какой компонент скорее всего неисправен?
А) Видеокарта
Б) Блок питания
В) Процессор
Г) Оперативная память
3. Прочитайте текст и запишите развернутый ответ. Системный администратор проводит плановое техническое обслуживание рабочей станции. При проверке состояния жесткого диска с помощью утилиты SMART он обнаружил, что один из атрибутов (количество переназначенных секторов) достиг критического порога. Пользователь сообщил, что система иногда зависает при работе с большими файлами, но перезагрузка временно помогает. Какие действия должен предпринять администратор для предотвращения потери данных и восстановления надежной работы системы?
4. Прочитайте текст и запишите ответ. Системный блок потребляет от сети переменного тока мощность 450 Вт при напряжении 220 В. Коэффициент мощности (cos φ) блока питания составляет 0,75. Определите силу тока (в амперах), потребляемую системным блоком из сети. Разрешается использовать калькулятор. В ответе укажите целую часть числа.
5. Прочитайте текст и запишите ответ. На жестком диске объемом 2 Тбайт занято 65 % пространства. Сколько гигабайт свободного места остается на диске? (Считайте, что 1 Тбайт = 1024 Гбайт). Разрешается использовать калькулятор. В ответе укажите целую часть числа.
6. Прочитайте текст и запишите развернутый ответ. В защищенной информационной системе, использующей аппаратные токены для аутентификации и электронной подписи, произошел сбой питания во время записи ключевой информации на токен. После восстановления питания пользователь не может войти в систему – токен не распознается, а система выдает ошибку «Неверный PIN-код» (хотя PIN вводится правильно). Резервная копия ключей хранится на защищенном сервере. Каков алгоритм действий специалиста по восстановлению работоспособности учетной записи пользователя с сохранением всех требований безопасности?
7. Прочитайте текст и запишите развернутый ответ. В организации принято решение о переходе на новую модель серверных накопителей с интерфейсом NVMe. При этом старое серверное оборудование поддерживает только SATA-диски. Техническому специалисту поручено модернизировать систему хранения данных без полной замены серверов. Доступны RAID-контроллер с поддержкой SATA и возможность установки PCIe-адаптера для NVMe-накопителей. Какое техническое решение является правильным и экономически обоснованным? Сравните возможные варианты подключения NVMe-накопителей к старому серверу.
8. Прочитайте текст и запишите ответ. Скорость передачи данных по каналу связи составляет 100 Мбит/с. Файл объемом 750 Мбайт необходимо передать по этому каналу. Сколько секунд займет передача файла? (Считайте, что 1 Мбайт = 8 Мбит). Разрешается использовать калькулятор.
9. Прочитайте текст и запишите ответ. Для организации RAID-массива уровня 5 используются три жестких диска по 4 Тбайт каждый. Определите полезную емкость массива (в Тбайт), доступную для хранения данных, без учета служебных областей. Разрешается использовать калькулятор.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
10. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Для защиты информации от утечки через побочные электромагнитные излучения наиболее эффективным пассивным средством является:
А) Установка генератора шума в помещении
Б) Использование экранированных кабелей и заземления
В) Регулярная смена паролей доступа
Г) Шифрование данных на жестком диске
11. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Какое действие является обязательным при замене материнской платы в системе с установленным программно-аппаратным средством защиты информации (СЗИ)?
А) Переустановка операционной системы с нуля
Б) Обновление прошивки всех периферийных устройств
В) Импорт резервных копий ключей и сертификатов СЗИ на новую платформу
Г) Отключение системы вентиляции на время замены

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
12. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор.При плановом техническом обслуживании рабочей станции обнаружено, что температура процессора под нагрузкой достигает критических значений. Какова наиболее вероятная причина?
А) Недостаточная мощность блока питания
Б) Высохшая термопаста или слабый прижим радиатора

В) Неисправность модуля оперативной памяти
Г) Сбой в работе операционной системы
13. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Для организации отказоустойчивого хранения данных, позволяющего выдержать отказ любого одного диска, но при этом обеспечивающего высокую скорость записи, наиболее подходит:
А) RAID 0
Б) RAID 1
В) RAID 5
Г) Простое копирование данных вручную на внешний диск
14. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При восстановлении работоспособности защищенной системы после аппаратного сбоя, в каком порядке следует выполнять проверку?
А) Сначала запустить прикладное ПО, затем проверить СЗИ
Б) Сначала проверить работу СЗИ и целостность ключей, затем тестировать общую производительность
В) Сначала заменить все кабели, затем подключить питание
Г) Сначала переустановить драйверы всех устройств, затем загрузить ОС
15. Прочитайте текст и запишите развернутый ответ. При проведении проверки эффективности защиты от ПЭМИН в помещении обработки конфиденциальной информации специалист обнаружил, что экранирующая оплетка на кабеле, соединяющем системный блок с монитором, имеет механические повреждения (перегибы и разрывы). Помещение не оборудовано активными средствами защиты (генераторами шума). Оцените степень риска утечки информации и предложите комплекс мер (включая временные и долгосрочные) для устранения выявленного недостатка.

Индикатор ИМЕТЬ НАВЫКИ И (ИЛИ) ОПЫТ ДЕЯТЕЛЬНОСТИ

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
1. Прочитайте текст и запишите развернутый ответ. При проведении ежемесячного технического обслуживания сервера администратор обнаружил, что один из вентиляторов в блоке питания издает посторонний шум и периодически останавливается. Сервер работает круглосуточно и содержит критически важную базу данных. Запасного блока питания в наличии нет. Какие действия должен предпринять администратор для минимизации риска выхода сервера из строя до момента замены блока питания?
2. Прочитайте текст и запишите развернутый ответ. В офисном помещении установлено 10 автоматизированных рабочих мест. При проведении замеров уровня электромагнитных излучений выявлено превышение допустимых норм вблизи одной из рабочих станций. При этом на других станциях аналогичной конфигурации превышений нет. Каковы возможные причины локального превышения и какие диагностические мероприятия необходимо провести для их выявления?
3. Прочитайте текст и запишите ответ. Блок питания компьютера имеет мощность 650 Вт и КПД 85 %. Определите мощность (в ваттах), фактически потребляемую блоком питания от электрической сети. Разрешается использовать калькулятор. В ответе запишите целую часть числа.
4. Прочитайте текст и запишите ответ. Объем системного диска составляет 512 Гбайт. Операционная система и установленное ПО занимают 180 Гбайт. Пользовательские данные занимают еще 95 Гбайт. Сколько процентов дискового пространства осталось свободным? (Ответ округлите до целого числа процентов). Разрешается использовать калькулятор. В ответе запишите целую часть числа.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
5. Прочитайте текст и запишите развернутый ответ. Сотрудник отдела информационной безопасности сообщил, что при попытке запуска защищенного приложения на рабочей станции появляется ошибка «Сертификат пользователя не найден» или «Не удалось получить доступ к закрытому ключу». При этом другие пользователи на аналогичных станциях работают нормально. Каковы вероятные причины возникновения ошибки и в какой последовательности следует выполнять проверки для восстановления доступа?
6. Прочитайте текст и запишите развернутый ответ. В системе хранения данных на основе RAID-массива уровня 5, состоящего из пяти дисков, один из дисков вышел из строя. Администратор заменил его на новый, но в процессе ребилда (восстановления) на втором диске стали появляться ошибки чтения. Каковы риски для целостности данных в сложившейся ситуации и какие действия должен предпринять администратор для минимизации потерь?
7. Прочитайте текст и запишите ответ. Скорость записи на SSD-накопитель составляет 550 Мбайт/с. Сколько времени (в секундах) потребуется для записи файла размером 11 Гбайт на этот накопитель? (Считайте, что 1 Гбайт = 1024 Мбайт). Разрешается использовать калькулятор. В ответе запишите целую часть числа.
8. Прочитайте текст и запишите ответ. Для резервного копирования используется внешний накопитель емкостью 4 Тбайт. Ежедневный объем резервируемых данных составляет 120 Гбайт. Сколько полных резервных копий можно разместить на накопителе, если хранить их без перезаписи? (Считайте, что 1 Тбайт = 1024 Гбайт). Разрешается использовать калькулятор. В ответе запишите целую часть числа.

ИТОГОВЫЙ ТЕСТ

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
1. Какие устройства относятся к средствам долговременного хранения информации в автоматизированной системе?
А) Жесткий диск (HDD)

Б) Твердотельный накопитель (SSD)
В) Оперативная память (RAM)
Г) Кэш-память процессора
2. Какие функции выполняет система BIOS/UEFI при включении компьютера?
А) Загрузка операционной системы с установленного носителя
Б) Инициализация и тестирование оборудования (POST)
В) Управление энергопотреблением процессора во время работы
Г) Предоставление интерфейса для настройки параметров аппаратного обеспечения
3. Какие уровни RAID обеспечивают отказоустойчивость системы при отказе одного диска?
А) RAID 0
Б) RAID 1
В) RAID 5
Г) RAID 10

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
4. Какие меры относятся к пассивным средствам защиты информации от утечки по техническим каналам?
А) Экранирование соединительных кабелей
Б) Генерация широкополосного шума
В) Заземление оборудования
Г) Использование ферритовых фильтров на кабелях
5. Какие компоненты проверяются в первую очередь при диагностике «синего экрана смерти» (BSOD), вызванного аппаратной проблемой?
А) Оперативная память
Б) Блок питания
В) Модуль TPM
Г) Накопитель (HDD/SSD)
6. Какие устройства используются для усиления аутентификации пользователя в защищенных информационных системах?
А) USB-токен
Б) Смарт-карта
В) Сканер отпечатков пальцев
Г) Сетевой коммутатор
7. Какие задачи решаются при проведении планового технического обслуживания рабочей станции?
А) Очистка внутреннего пространства от пыли
Б) Установка нового антивирусного ПО
В) Проверка надежности крепления компонентов
Г) Обновление драйверов всех устройств
8. Какие признаки характерны для неисправности блока питания?
А) Компьютер не включается при нажатии кнопки питания
Б) При работе компьютер внезапно перезагружается под нагрузкой
В) На экране появляется сообщение о недостатке оперативной памяти
Г) Системные вентиляторы не вращаются, но индикаторы горят

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
9. Какие действия должны быть выполнены после замены вышедшего из строя накопителя в защищенной системе?
А) Восстановление данных из резервной копии
Б) Переустановка операционной системы
В) Импорт криптографических ключей и сертификатов
Г) Настройка порядка загрузки устройств в BIOS/UEFI
10. Какие каналы утечки информации относятся к техническим каналам (не связанным с человеческим фактором)?
А) Побочные электромагнитные излучения (ПЭМИН)
Б) Акустические колебания в помещении
В) Наводки на линии электропитания
Г) Социальная инженерия
11. Какие параметры системы охлаждения необходимо контролировать при диагностике перегрева оборудования?
А) Температура процессора
Б) Температура чипсета материнской платы
В) Температура воздуха в помещении
Г) Уровень шума вентиляторов
12. Какие средства относятся к аппаратной криптографической защите информации?
А) Аппаратный генератор случайных чисел
Б) Криптографический сопроцессор процессора
В) USB-токен для хранения ключей
Г) Программный криптопровайдер OpenSSL
13. Какие действия следует предпринять при обнаружении «битых» секторов на жестком диске по результатам

диагностики?
А) Сделать резервную копию всех важных данных
Б) Заменить жесткий диск на новый
В) Запустить дефрагментацию диска
Г) Попытаться восстановить данные с помощью специализированного ПО
14. Какие функции выполняет модуль TPM (Trusted Platform Module) в составе защищенной системы?
А) Хранение и генерация криптографических ключей
Б) Контроль целостности загружаемой операционной системы
В) Ускорение вычислений видеокарты
Г) Защита от перегрева процессора
15. Какие документы должны быть оформлены по итогам восстановления работоспособности автоматизированной системы после отказа?
А) Акт ввода системы в эксплуатацию после ремонта
Б) Дефектная ведомость (заключение о причинах отказа)
В) Договор на гарантийное обслуживание оборудования
Г) Журнальная запись о проведенном ремонте и времени простоя

Темы индивидуальных проектов, курсовых работ (проектов), индивидуальных заданий на практику:

Учебным планом не предусмотрено

Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ	ПОРОГОВЫЙ УРОВЕНЬ	ПРОДВИНУТЫЙ УРОВЕНЬ	ВЫСОКИЙ УРОВЕНЬ
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «незачет», «неудовлетворительно»	Оценка «зачтено/удовлетворительно» ,«удовлетворительно»	Оценка «зачтено/хорошо», «хорошо»	Оценка «зачтено/отлично», «отлично»

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

Недостаточный уровень:
Знает отдельные элементы профессионального контекста (название профессии, отдельные виды задач), может перечислить 1-2 этапа плана решения задачи по образцу, называет 1-2 источника информации (учебник, интернет), а также знает один способ оценки результата («правильно/неправильно»).

Умеет под руководством преподавателя распознавать простейшую задачу в знакомой профессиональной ситуации, выделять 1-2 очевидные составные части задачи, определять этапы решения по образцу, искать

Умеет под руководством преподавателя распознавать простейшую задачу в знакомой профессиональной ситуации, выделять 1-2 очевидные составные части задачи, определять этапы решения по образцу, искать информацию в одном заданном источнике (учебник, конспект), составлять простейший план из 2-3 шагов по шаблону, определять минимальные ресурсы (время, материалы) при прямой подсказке, выполнять план строго по инструкции, а также оценивать результат по критерию «сделано/не сделано» с помощью наставника.

Пороговый уровень:
Знает актуальный профессиональный контекст (основные виды профессиональных задач, типовые условия их выполнения, требования к результату) и социальный контекст (нормы профессиональной коммуникации, базовые этические принципы), структуру плана решения задач (цель, этапы, ресурсы, сроки), алгоритмы выполнения типовых работ в профессиональной области, основные источники информации (нормативные документы, справочные системы, профессиональные сайты), методы работы в профессиональной сфере, а также порядок оценки результатов решения задач (критерии, способы измерения, формы фиксации).

Умеет самостоятельно распознавать задачу или проблему в типовом профессиональном и социальном контексте, анализировать задачу с выделением основных составных частей (условия, ограничения, требования), определять логические этапы решения задачи, выявлять и эффективно искать необходимую информацию в нескольких типовых источниках (нормативные документы, справочные системы, профессиональные сайты), составлять развёрнутый план действий с указанием последовательности шагов, определять необходимые ресурсы (временные, материальные, информационные, человеческие), владеть актуальными методами работы в профессиональной сфере, реализовывать составленный план, а также оценивать результат и ближайшие последствия своих действий с обоснованием по заданным критериям.

Продвинутый уровень:
Знает изменчивый и многовариантный характер профессионального и социального контекста (включая нестандартные ситуации, конфликт интересов, межведомственное взаимодействие), структуру развёрнутого плана решения задач с учётом рисков и альтернатив, алгоритмы выполнения работ не только в профессиональной, но и в смежных областях, расширенный перечень источников информации (включая базы данных, экспертные заключения, профессиональные форумы), разнообразные методы работы в профессиональной и смежных сферах, а также порядок оценки результатов с учётом различных групп критериев (качество, эффективность, безопасность, экономичность).

Умеет самостоятельно распознавать проблему в нестандартном профессиональном или социальном контексте (в том числе при неполной или противоречивой информации), анализировать проблему с выделением скрытых составных частей (латентные ограничения, неявные требования, потенциальные риски), определять этапы решения задачи с учётом возможных альтернатив и точек ветвления, выявлять и эффективно искать информацию в разнородных источниках (включая экспертные заключения, базы данных, профессиональные форумы, нормативно-правовые акты), составлять развёрнутый план действий с альтернативными вариантами и резервными шагами, определять необходимые ресурсы с учётом их ограниченности и взаимозаменяемости, владеть актуальными методами работы в профессиональной и смежных сферах (включая комбинирование методов), гибко реализовывать составленный план с корректировкой по ходу выполнения, а также оценивать результат и последствия своих действий (краткосрочные и долгосрочные) с прогнозированием возможных эффектов.

Высокий уровень:
Знает методологию анализа динамического профессионального и социального контекста (включая глобальные тренды, отраслевые изменения, социокультурные факторы), структуру стратегического плана решения задач с интеграцией множественных альтернатив и сценариев, алгоритмы выполнения работ в профессиональной и смежных областях с возможностью их параметрической настройки, исчерпывающий перечень источников информации (включая научные публикации, открытые API, экспертные системы), передовые методы работы в профессиональной и смежных сферах (включая междисциплинарные подходы), а также порядок оценки результатов решения задач с использованием методов системного анализа, риск-менеджмента и экономической оценки.

Умеет самостоятельно распознавать и формулировать проблемы в слабо структурированном, динамично меняющемся профессиональном или социальном контексте (включая междисциплинарные и инновационные области), проводить глубокий многоаспектный анализ проблемы с выделением всех её составных частей (включая системные связи, причинно-следственные цепочки, латентные противоречия), определять этапы решения задачи с построением сценариев развития ситуации, выявлять и эффективно искать информацию с использованием современных информационно-аналитических систем (включая открытые API, наукометрические базы данных, экспертные системы), составлять стратегический план действий с множественными сценариями, точками принятия решений и механизмами обратной связи, определять необходимые ресурсы с учётом динамики их поступления и использования, владеть передовыми методами работы в профессиональной и смежных сферах (включая инновационные и авторские методики), реализовывать составленный план в условиях высокой неопределённости с непрерывным мониторингом и адаптацией, а также оценивать результат и последствия своих действий с использованием методов системного анализа, риск-менеджмента и стоимостной оценки.

ПК 1.4.: Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении

Умеет под руководством преподавателя выполнять перезагрузку компьютера, проверять подключение кабелей, запускать встроенную диагностику (POST), интерпретировать звуковые сигналы BIOS по таблице, а также заменять простой расходный материал (батарейка CMOS, кабель).

Знает отдельные понятия (техническое обслуживание, профилактика, диагностика), может назвать 1-2 вида обслуживания (ежедневное, плановое), понимает важность чистки и проверки оборудования, знает, что нужно удалять пыль и проверять соединения.

Имеет практический опыт просмотра журнала событий антивируса по инструкции, перезапуска службы СЗИ под контролем, проверки статуса лицензии по образцу, а также выполнения восстановления конфигурации из резервной копии по шаблону.

Пороговый уровень:
Умеет самостоятельно обеспечивать работоспособность технических средств (профилактика, мониторинг температуры и SMART), обнаруживать неисправности (визуальный осмотр, анализ журналов событий, запуск диагностических утилит (memtest, проверка диска, тест стабильности)), устранять типовые неисправности (перезагрузка, замена кабелей, переустановка драйверов, замена компонентов (блок питания, память, диск, кулер), восстановление ПО, настройка BIOS, обновление драйверов и прошивок), а также проверять работоспособность после устранения и вести документацию.

Знает принципы основных методов организации и проведения технического обслуживания (ТО) вычислительной техники и технических средств информатизации: виды ТО (ежедневное, планово-предупредительное (ППР), сезонное, обслуживание по состоянию, по регламенту); методы ТО (профилактический, диагностический, восстановительный, ремонтный); порядок организации ТО (планирование, подготовка, выполнение, учёт, контроль); основные регламентные работы (чистка от пыли, проверка систем охлаждения, диагностика компонентов (процессор, память, диск, блок питания), проверка электропитания, заземления, обновление ПО и прошивок, тестирование работоспособности, замена расходных материалов); а также правила техники безопасности при проведении ТО.

Имеет практический опыт диагностики компонентов СЗИ (журналы, тестирование, целостность, обновления, политики), устранения типовых отказов (перезапуск служб, восстановление конфигураций, переустановка, корректировка политик, замена сертификатов/лицензий, откат обновлений), а также восстановления работоспособности АС в защищённом исполнении (восстановление из резервной копии, проверка целостности, аудит, документирование) с соблюдением требований нормативных документов.

Продвинутый уровень:
Знает детальные методики ППР для различных типов оборудования (серверы, рабочие станции, сетевое оборудование, СХД, периферия), методы прогнозирования отказов на основе мониторинга (температура, SMART, частота ошибок), способы организации ТО в критических инфраструктурах (горячая замена, резервирование), а также требования нормативных документов к периодичности и объёму ТО (ГОСТ, ведомственные нормы).

Умеет самостоятельно проводить углублённую диагностику для серверов, СХД и сетевого оборудования (анализ логов SMART, ECC, журналов RAID), прогнозировать отказы на основе данных мониторинга, устранять сложные неисправности (восстановление BIOS, перепрошивка контроллеров, замена компонентов на материнской плате (конденсаторы, MOSFET), восстановление RAID-массивов), а также применять методы горячей замены и резервирования для обеспечения работоспособности в критических инфраструктурах.

Имеет практический опыт углублённой диагностики для различных типов СЗИ (СКЗИ, DLP, IDS/IPS, EDR, SIEM), устранения сложных отказов (восстановление базы данных политик, синхронизация ключей, устранение конфликтов с системными обновлениями, восстановление криптоконтейнеров), а также восстановления работоспособности АС в защищённом исполнении после инцидентов (компрометация, атака) с применением мер форензики.

Высокий уровень:
Имеет практический опыт внедрения автоматизированной диагностики и самовосстановления СЗИ (DevSecOps, AI/ML), проектирования стратегий обеспечения отказоустойчивости и непрерывности защищённых АС, анализа корневых причин сложных отказов, восстановления систем после APT-атак, а также обучения других диагностике, устранению отказов и восстановлению защищённых АС.

Умеет самостоятельно внедрять предиктивную диагностику (AI/ML, анализ больших данных), автоматизировать обнаружение и устранение неисправностей (скрипты, откат, переключение на резерв), проектировать стратегии обеспечения работоспособности для распределённых и высоконагруженных систем, проводить анализ корневых причин отказов, а также обучать других методам обеспечения работоспособности, обнаружения и устранения неисправностей.

Знает методологию оптимизации системы ТО на основе анализа надёжности и экономической эффективности, современные подходы к автоматизации ТО (мониторинг, удалённая диагностика, предиктивная аналитика), принципы построения систем управления ТО (CMMS, ITIL), а также стратегии технического обслуживания для высокодоступных и территориально распределённых систем.

ПК 2.1.: Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации

Недостаточный уровень:
Знает отдельные названия средств защиты информации (антивирус, брандмауэр, пароль), понимает назначение

Знает отдельные названия средств защиты информации (антивирус, брандмауэр, пароль), понимает назначение защиты в ОС, сети, БД, знает 1-2 способа применения (запуск сканирования, настройка прав доступа), а также знает, что такое лицензия и обновление.

Умеет под руководством преподавателя запускать установку антивируса, следовать инструкциям установщика (нажимать «Далее»), вводить лицензионный ключ по образцу, а также включать базовую защиту (брандмауэр) по инструкции.

Имеет практический опыт запуска установки антивируса по инструкции, следования указаниям установщика (нажатие «Далее») под контролем, ввода лицензионного ключа по образцу, а также выполнения базовой настройки (включение защиты, планирование сканирования) по шаблону.

Пороговый уровень:
Знает особенности и способы применения программных и программно-аппаратных средств защиты информации: классификацию СЗИ (антивирусные средства, межсетевые экраны (FW/UTM/NGFW), средства контроля доступа (локальные/доменные), средства криптографической защиты (СКЗИ), средства анализа защищённости (сканеры уязвимостей), средства обнаружения вторжений (IDS/IPS), DLP-системы, средства резервного копирования, средства аутентификации (парольная, двухфакторная, биометрическая)); особенности применения в операционных системах (настройка политик безопасности, контроль учётных записей, аудит, шифрование дисков (BitLocker, LUKS), мандатный контроль (SELinux, AppArmor)); особенности применения в компьютерных сетях (сегментация, межсетевые экраны, VPN, фильтрация трафика, IDS/IPS, прокси-серверы); особенности применения в базах данных (разграничение доступа на уровне таблиц/строк/столбцов, шифрование данных, аудит запросов, контроль привилегий, средства защиты от SQL-инъекций); а также способы настройки и эксплуатации типовых СЗИ в каждой из сред.

Умеет самостоятельно устанавливать программные и программно-аппаратные средства защиты информации (антивирус, брандмауэр, СКЗИ, контроль доступа, DLP, IDS/IPS), выполнять базовую настройку (политики сканирования, правила фильтрации, права доступа, ключи и сертификаты), применять СЗИ по назначению (обнаружение угроз, блокировка, аудит, шифрование), проверять совместимость и лицензирование, а также обновлять базы и версии.

Имеет практический опыт установки программных средств защиты информации в автоматизированной системе (антивирус, брандмауэр, контроль доступа, СКЗИ, DLP, IDS/IPS, резервное копирование), настройки в соответствии с требованиями (политики, правила, права, ключи, сигнатуры), проверки совместимости и лицензирования, тестирования работоспособности после установки и настройки, а также документирования выполненных работ.

Продвинутый уровень:
Знает детальные особенности применения сертифицированных СЗИ для различных классов защищённости, способы интеграции СЗИ между собой (SIEM, оркестрация), методы обхода и противодействия обходу СЗИ, особенности защиты в виртуальных и облачных средах, а также требования нормативных документов (ФСТЭК, ФСБ) к применению СЗИ.

Умеет самостоятельно устанавливать и настраивать сертифицированные СЗИ для различных ОС (Windows, Linux, Astra Linux) и классов защищённости, настраивать СЗИ в виртуальных средах и сетевых архитектурах (кластеры, филиалы), оптимизировать настройки под производительность и профили угроз, а также тестировать работоспособность СЗИ после установки и настройки.

Имеет практический опыт установки и настройки сертифицированных программных СЗИ для различных классов защищённости АС, настройки СЗИ в виртуальных средах и распределённых АС, оптимизации настроек под производительность и профиль угроз, выполнения тестирования и ввода в эксплуатацию по требованиям ФСТЭК, а также устранения проблем совместимости и производительности.

Высокий уровень:
Знает современные архитектуры СЗИ (EDR, XDR, NGFW с IPS, UEBA, SOAR), методы применения AI/ML в СЗИ, стратегии защиты для КИИ и государственных информационных систем, особенности защиты в распределённых гетерогенных средах, а также методологию выбора и обоснования СЗИ под профиль угроз.

Умеет самостоятельно автоматизировать установку и настройку СЗИ (DevSecOps, Infrastructure as Code, Ansible, групповые политики), управлять конфигурациями СЗИ в гетерогенных и распределённых средах, выполнять бесшовное обновление и миграцию СЗИ, интерпретировать требования нормативных документов (ФСТЭК, ФСБ) для государственных информационных систем и КИИ, а также обучать других установке, настройке и применению СЗИ.

Имеет практический опыт автоматизации установки и настройки программных СЗИ в АС (DevSecOps, Infrastructure as Code, Ansible, групповые политики), управления конфигурациями и жизненным циклом СЗИ в гетерогенных и распределённых АС, выполнения бесшовного обновления и миграции СЗИ в защищённых средах, интерпретации требований нормативных документов для государственных информационных систем и КИИ, а также обучения других установке и настройке программных СЗИ.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

5.1.1. Основная литература

Л.1.1	Тюрин И. В. Вычислительная техника и информационные технологии [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2023. - 336 с. – Режим доступа: https://e.lanbook.com/book/339764
Л.1.2	Тюрин И. В. Вычислительная техника [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2023. - 296 с. – Режим доступа: https://e.lanbook.com/book/351881
Л.1.3	Акимова Е. В. Вычислительная техника. [Электронный ресурс]:учебное пособие для спо.. - Санкт-Петербург: Лань, 2022. - 68 с. – Режим доступа: https://e.lanbook.com/book/185888
Л.1.4	Тюрин И. В. Вычислительная техника и информационные технологии [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2024. - 336 с. – Режим доступа: https://e.lanbook.com/book/359855
Л.1.5	Нестеров С. А. Основы информационной безопасности [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2022. - 324 с. – Режим доступа: https://e.lanbook.com/book/206279
Л.1.6	Акимова Е. В. Вычислительная техника [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2023. - 68 с. – Режим доступа: https://e.lanbook.com/book/306785
Л.1.7	Лохов В. И., Петренко В. И., Мандрица И. В., Максименко Ю. К. Технические средства защиты информации. Лабораторный практикум. Technical means of information protection. Laboratory practicals [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2024. - 480 с. – Режим доступа: https://e.lanbook.com/book/434159
Л.1.8	Лебедев С. Г. Технические средства информатизации [Электронный ресурс]:учебное пособие для контактной и самостоятельной работы студентов, обучающихся по специальности 09.02.07 информационные системы и программирование, очной формы обучения. - пос. Караваево: КГСХА, 2024. - 48 с. – Режим доступа: https://e.lanbook.com/book/511388
Л.1.9	Безик В. А. Технические средства обеспечения безопасности [Электронный ресурс]:учебно-методическое пособие по выполнению лабораторных работ по дисциплине «технические средства обеспечения безопасности автоматизированных производств» для студентов направления подготовки 15.03.04 автоматизация технологических процессов и производств. - Брянск: Брянский ГАУ, 2024. - 38 с. – Режим доступа: https://e.lanbook.com/book/513272
Л.1.10	Карпенков С. Х. Технические средства информационных технологий [Электронный ресурс]:учебное пособие. - Москва: Директ-Медиа, 2023. - 376 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=707511
Л.1.11	Смирнов Ю. А. Технические средства автоматизации и управления [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2023. - 456 с. – Режим доступа: https://e.lanbook.com/book/355340
5.1.2. Дополнительная литература	
Л.2.1	Советов Б. Я., Цехановский В. В. Информационные технологии: теоретические основы [Электронный ресурс]:учебник для спо. - Санкт-Петербург: Лань, 2021. - 444 с. – Режим доступа: https://e.lanbook.com/book/153674
Л.2.2	Журавлев А. Е. Организация и архитектура ЭВМ. Вычислительные системы [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2020. - 144 с. – Режим доступа: https://e.lanbook.com/book/149338
5.2. Перечень программного обеспечения	
Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition	
5.3. Перечень информационных справочных систем	
Электронно-библиотечная система "Университетская библиотека онлайн" Электронно-библиотечная система "Лань" "Электронная библиотека учебников"	

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1312 - Лаборатория Учебная аудитория для проведения занятий лекционного типа, лабораторных и практических занятий; занятий семинарского типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Маркерная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Учебно-наглядные пособия
Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1310 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Ноутбук переносной; Переносной проектор; Переносной экран; Учебно-наглядные пособия
Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1302 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочее место преподавателя; маркерная доска; 10 рабочих мест обучающихся, оснащенных ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду;

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Методические рекомендации по организации самостоятельной работы

СРС – планируемая учебная, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (возможно частичное непосредственное участие преподавателя при сохранении ведущей роли студентов). Целью СРС является овладение фундаментальными знаниями, профессиональными умениями и навыками по профилю будущей специальности, опытом творческой, исследовательской деятельности, развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровней. Задачи СРС: систематизация и закрепление полученных теоретических знаний и практических умений студентов; углубление и расширение теоретической подготовки; формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу; развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации; развитие исследовательских умений; использование материала, собранного и полученного в ходе самостоятельных занятий на практических занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к текущей и промежуточной аттестации. Функции СРС: развивающая (повышение культуры умственного труда, приобщение к 10 творческим видам деятельности, обогащение интеллектуальных способностей студентов); информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится мало результативной); ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация); воспитательная (формируются и развиваются профессиональные качества специалиста и гражданина); исследовательская (новый уровень профессионально-творческого мышления).

Самостоятельная работа студентов является обязательным компонентом учебного процесса для каждого студента и определяется учебным планом. Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем. Самостоятельная работа – это познавательная учебная деятельность, когда последовательность мышления студента, его умственных и практических операций и действий зависит и определяется самим студентом.

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня, что в итоге приводит к развитию навыка самостоятельного планирования и реализации деятельности. Целью самостоятельной работы студентов является овладение необходимыми компетенциями по своему направлению подготовки, опытом творческой и исследовательской деятельности. На основании компетентностного подхода к реализации профессиональных образовательных программ, видами заданий для самостоятельной работы являются:

- для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и информационно-телекоммуникационной сети Интернет и др.
- для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей), повторная работа над учебным материалом, составление плана, составление таблиц для систематизации учебного материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др.), завершение аудиторных практических работ и оформление отчётов по ним, подготовка мультимедиа сообщений/докладов к выступлению на семинаре (конференции), материалов-презентаций, подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.
- для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, выполнение расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Методические рекомендации по освоению дисциплины (учебного предмета)

Методические рекомендации по подготовке к лекционным занятиям

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Работа с рекомендованной литературой:

При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала.

Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:
- план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения,
- текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника,
- свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом,
- тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу. В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации по подготовке к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки теоретического материала предмета путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к практическим занятиям включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение практического занятия предполагает, например:
 индивидуальные выступления студентов с сообщениями по какому-либо вопросу изучаемой темы;
 фронтальное обсуждение рассматриваемой проблемы, обобщения и выводы;
 решение задач и упражнений по образцу;
 решение вариантных задач и упражнений;
 решение ситуационных производственных (профессиональных) задач;
 проектирование и моделирование разных видов и компонентов профессиональной деятельности.
 выполнение контрольных работ;
 работу с тестами.
При подготовке к практическим занятиям студентам рекомендуется: внимательно ознакомиться с тематикой практического занятия; прочесть конспект лекции по теме, изучить рекомендованную литературу;
составить краткий план ответа на каждый вопрос практического занятия; проверить свои знания, отвечая на вопросы для самопроверки; если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради.
Все письменные задания выполнять в рабочей тетради. Практические занятия развивают у студентов навыки самостоятельной работы по решению конкретных задач.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине. Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:
 изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
 выполнение необходимых расчетов и экспериментов;
 оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;
 по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала. Контроль усвоения теоретического материала является индивидуальным.

Методические указания по выполнению отчёта к лабораторным работам

Основным требованием по выполнению лабораторных и практических работ является полное исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения и профессиональной подготовки студентов.
Методические указания обеспечивают комплексный подход в учебной работе студентов, единство и преемственность требований к оформлению результатов работы на разных этапах обучения. С единых позиций приведены основные требования по структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.
Дополнительными элементы:
- приложения;
- библиографический список.
Требования к содержанию отчёта:
1. Титульный лист
В верхнем поле листа указывают полное наименование учебного заведения.
В среднем поле указывается вид работы, в данном случае лабораторная или практическая работа с указанием курса, по которому она выполнена, и ниже ее название. Название работы приводится без слова тема и в кавычки не заключается.

Далее ближе к правому краю титульного листа указывают фамилию, инициалы и группу учащегося, выполнившего работу, а также фамилию, инициалы преподавателя, принявшего работу.
В нижнем поле листа указывается место выполнения работы и год ее написания (без слова год).
2. Цель работы должна отражать тему работы, а также конкретные задачи, поставленные студенту на период выполнения работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.
3. Краткие теоретические сведения. В этом разделе излагается краткое теоретическое описание изучаемой в работе темы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий, требующихся для дальнейшей обработки полученных результатов. Объем литературного обзора не должен превышать 1/3 части всего отчета.
4. Ход выполнения работы. В данном разделе подробно излагается методика выполнения работы, процесс получения данных и способ их обработки. Если используются стандартные пакеты компьютерных программ для обработки экспериментальных результатов, то необходимо обосновать возможность и целесообразность их применения, а также подробности обработки данных с их помощью.
5. Выводы по работе - кратко излагаются результаты работы, полученные в результате выполнения работы, а также краткий анализ полученных результатов.
Для защиты лабораторной работы студент должен подготовить отчет, провести самостоятельную работу, иметь отметку о проверенном отчете.
Результаты определяются по пятибалльной системе оценок.

Методические рекомендации по выполнению реферата

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы. Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора. Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и для каких целей их использует. Требования к языку реферата.
Должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата:
1. Титульный лист
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных. Общие требования к построению, содержанию и оформлению».
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Методические рекомендации по устному опросу/самоподготовке

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов, воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств. В случае необходимости следует рекомендовать еще раз внимательно разобраться в материале. Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение решать задачи или пройти тестирование по пройденному материалу. Однако преподавателю следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Методические рекомендации по подготовке к семинарским занятиям

Одним из видов внеаудиторной самостоятельной работы является подготовка к семинарским занятиям. Семинар –

форма учебно-практических занятий, при которой студенты обсуждают сообщения, доклады и рефераты, выполненные ими по результатам учебных или научных исследований под руководством преподавателя. Преподаватель в этом случае является координатором обсуждений темы семинара, подготовка к которому является обязательной. Поэтому тема семинара и основные источники обсуждения предъявляются до обсуждения для детального ознакомления, изучения. Цели обсуждений направлены на формирование навыков профессиональной полемики и закрепление обсуждаемого материала. Семинар – это такая форма организации обучения, при которой на этапе подготовки доминирует самостоятельная работа учащихся с
учебной литературой и другими дидактическими средствами над серией вопросов, проблем и задач, а в процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, где они под руководством преподавателя делают обобщающие выводы и заключения. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания, то главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли.

Методические рекомендации по подготовке эссе

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (эссе) представляет собой оригинальное произведение объемом 500-700 слов, посвященное какой-либо значимой классической либо современной проблеме в определенной теоретической и практической области. Творческая работа не является рефератом и не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно способствовать раскрытию творческих и аналитических способностей. Цели написания эссе – научиться логически верно и аргументировано строить устную и письменную речь;
работать над углублением и систематизацией своих философских знаний; овладеть способностью использовать основы знаний для формирования мировоззренческой позиции. Приступая к написанию эссе, изложите в одном предложении, что именно вы будете утверждать и доказывать (свой тезис).

Методические рекомендации по подготовке к докладу

Для подготовки доклада необходимо выбрать актуальную тему. Желательно, чтобы тема была интересна докладчику и вызывала желание качественно подготовить материалы. Подготовка доклада предполагает: определение цели доклада; подбор необходимого материала, определяющего содержание доклада; составление плана доклада, распределение собранного материала в необходимой логической последовательности.
Композиция доклада имеет вступление, основную часть и заключение.
Вступление должно содержать: название доклада; сообщение основной идеи; современную оценку предмета изложения; краткое перечисление рассматриваемых вопросов; интересную для слушателей форму изложения. Основная часть, в которой необходимо раскрыть суть темы, обычно строится по принципу отчёта. Задача основной части: представить достаточно данных для того, чтобы слушатели заинтересовались темой.
Заключение – чёткое обобщение и краткие выводы по излагаемой теме.

Методические рекомендации по подготовке к собеседованию

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.
Цель собеседования: проверка усвоения знаний; умений применять знания; сформированности профессионально значимых личностных качеств.
Подготовка к собеседованию предполагает повторение пройденного материала и приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины.

Методические рекомендации по подготовке к тестированию/ итоговому тестированию

Тестирование/итоговое тестирование – это система стандартизированных заданий, определенного содержания и упорядоченных в рамках определенной стратегии предъявления, позволяющая качественно оценить структуру и эффективно измерить уровень знаний, умений и навыков по учебной дисциплине (разделу). Тестирование/итоговое тестирование позволяет оценить у студентов уровень знаний фактического материала, умения логически мыслить, способности к рефлексии и творческому подходу к решению поставленной задачи на каждом этапе их обучения.
При самостоятельной подготовке к тестированию/итоговому тестированию студенту необходимо:
- четко выяснить все условия тестирования/итогового тестирования заранее (сколько тестов будет предложено, сколько времени отводится на тестирование/итоговое тестирование, какова система оценки результатов);
- проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- проработать информационный материал по разделу дисциплине;
- конспективно выписать из соответствующих разделов учебной дисциплины основные понятия, ключевые идеи, теоретические концепции и подходы;
- повторить теоретический материал лекций, самостоятельно изученной учебной и научной литературы, семинарских занятий.
При выполнении тестовых заданий рекомендуется:
- внимательно полностью прочитать вопрос и предлагаемые варианты ответов, выбрать правильные из них (их может быть несколько);
- при затруднении при ответе на сложный для студента вопрос целесообразно переходить к другим вопросам теста. По завершению ответов на все последующие вопросы теста необходимо вернуться к трудному вопросу и дать на него продуманный ответ;

- по окончании тестирования/итогового тестирования следует проверить правильность данных ответов на вопросы теста, чтобы избежать механических ошибок.

Методические рекомендации по подготовке к экзамену

Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине. Экзаменационная сессия – это серия экзаменов, установленных учебным планом. Между экзаменами интервал 2-4 дня, в течение студент систематизирует уже имеющиеся знания. На консультации перед экзаменом студенты должны
быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки вопросы. Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

Методические рекомендации по подготовке к зачету/ зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно- методической документацией:
- программой дисциплины;
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета/зачета с оценкой.

Методические рекомендации по выполнению курсовой работы/ курсового проекта

Курсовая работа/курсовой проект - это учебно-исследовательский труд студента, выполняемый по определённой дисциплине под руководством научного руководителя. Её цель - закрепить и углубить теоретические знания, развить навыки самостоятельного анализа, работы с научной литературой и эмпирическими данными, а также сформировать умения структурировать информацию и формулировать обоснованные выводы.
Курсовая работа/курсовой проект – письменная работа объемом 30–50 страниц, выполняется в несколько этапов:
1. Подготовительный этап
2. Сбор и анализ информации
3. Написание работы
Структура курсовой работы/курсового проекта:
1. Титульный лист – по шаблону вуза.
2. Содержание – разделы с номерами страниц.
3. Введение: актуальность, цель, задачи, объект, предмет, методы, значимость, структура.
4. Основная часть:
o Глава 1 (теоретическая) – анализ концепций, выводы.
o Глава 2 (аналитическая/практическая) – анализ объекта, расчёты, данные, выводы.
o Глава 3 (рекомендательная, если нужно) – предложения, прогнозы, выводы.
5. Заключение – выводы по задачам, итоги, перспективы.
6. Список литературы – группируйте по типам, оформляйте по ГОСТ, указывайте только использованные источники.
7. Приложения (если нужно) – таблицы, графики, анкеты и т. д. (нумеруются, есть ссылки в тексте).
4. Оформление
5. Проверка и доработка
6. Подготовка к защите
• Доклад (5–7 мин.):
• Презентация.

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.
Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей.
Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.
Основной формой в дистанционном обучении является индивидуальная форма обучения. Главным достоинством

индивидуального обучения для инвалидов и лиц с ограниченными возможностями здоровья является то, что оно позволяет полностью индивидуализировать содержание, методы и темпы учебной деятельности инвалида, следить за каждым его действием и операцией при решении конкретных задач; вносить вовремя необходимые коррекции как в деятельность студента-инвалида, так и в деятельность преподавателя. Дистанционное обучение также обеспечивает возможности коммуникаций не только с преподавателем, но и с другими обучаемыми, сотрудничество в процессе познавательной деятельности.
При изучении дисциплины используются следующие организационные мероприятия:

- использование возможностей сети «Интернет» для обеспечения связи с обучающимися, предоставления им необходимых материалов для самостоятельного изучения, контроля текущей успеваемости и проведения тестирования;

- проведение видеоконференций, лекций, консультаций, и т.д. с использованием программ, обеспечивающих дистанционный контакт с обучающимся в режиме реального времени.
- предоставление электронных учебных пособий, включающих в себя основной материал по дисциплинам, включенным в ОП;

- проведение занятий, консультаций, защит курсовых работ и т.д. на базе консультационных пунктов, обеспечивающих условия для доступа туда лицам с ограниченными возможностями;
- предоставление видеолекций, позволяющих изучать материал курса дистанционно.
- использование программного обеспечения и технических средств, имеющих функции адаптации для использования лицами с ограниченными возможностями.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2026 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2027 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2028 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2029 г. № __
Председатель ПЦК _____

==========