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
МДК.01.01 Операционные системы

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 **100 часов**

Часов по учебному плану 100

в том числе:

контактная работа 96

самостоятельная работа 4

Виды контроля в семестрах:

Контрольная работа - 3

Распределение часов дисциплины по семестрам

Вид учебной работы	Трудоемкость, часов			
	семестр 3		Итого	
	УП	РП	УП	РП
Лекции	48	48	48	48
Лабораторные	48	48	48	48
В т.ч. в форме практ. подгот.	4	4	4	4
Контактная работа	96	96	96	96
Сам. работа	4	4	4	4
Часы на контроль				

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 Долотовский Алексей Игоревич ___

Рабочая программа дисциплины
Операционные системы

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:	П

Дисциплина Операционные системы является частью неопознанный объект и обязательна для изучения.

Требования к предварительной подготовке обучающегося:	
1	Биология
2	География
3	Иностранный язык
4	Информатика
5	История
6	Литература
7	Математика
8	Обществознание
9	Основы безопасности жизнедеятельности
10	Русский язык
11	Физика
12	Физическая культура
13	Химия
14	Базовые дисциплины
15	Профильные дисциплины
Дисциплины (модули) и практики, для которых освоение данной дисциплины необходимо как предшествующее:	
1	Базы данных
2	Производственная практика (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)
3	Учебная практика (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)
4	Экзамен по модулю (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)
5	Защита информации техническими средствами
6	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих
7	Основы философии
8	Экологические основы природопользования
9	Организационно-правовое обеспечение информационной безопасности
10	Электроника и схемотехника
11	Экономика и управление
12	Безопасность жизнедеятельности
13	Технические средства информатизации
14	Экзамен по модулю "ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении"
15	Эксплуатация компьютерных сетей
16	Производственная практика по ПМ.01
17	Криптографические средства защиты информации
18	Производственная практика по ПМ.02
19	Техническая защита информации
20	Инженерно-технические средства физической защиты объектов информатизации
21	Учебная практика по ПМ.03
22	Производственная практика по ПМ.03
23	Квалификационный экзамен по "ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих"
24	Выполнение работ по должности "Оператор электронно-вычислительных и вычислительных машин"
25	Учебная практика по ПМ.04
26	Производственная практика по ПМ.04
27	Производственная практика (преддипломная)

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

Цели освоения: Формирование у студентов системных знаний о принципах работы операционных систем, архитектуре автоматизированных систем, а также практических навыков по конфигурированию, настройке и администрированию ОС в защищенном исполнении с учетом требований к защите информации, что обеспечивает готовность к выполнению профессиональных задач в области комплектования, настройки и сопровождения систем защиты информации.
Задачи: 1. Изучить состав, архитектуру и принципы функционирования современных операционных систем и сред.
2. Освоить методы разработки алгоритмов и приемов программирования системных компонентов.
3. Сформировать умения по комплектованию и конфигурированию автоматизированных систем в защищенном исполнении.
4. Привить практические навыки установки и настройки компонентов систем защиты информации (СЗИ) автоматизированных систем.
5. Научить студентов применять средства управления процессами, памятью, файловыми системами и устройствами ввода-вывода в контексте защищенных АС.
6. Развить навыки администрирования сетевых подсистем, межсетевых экранов и политик безопасности.
7. Обеспечить понимание подходов к аудиту, резервному копированию, восстановлению и аттестации защищенных систем.
Изучение дисциплины направлено на формирование у обучающихся следующих компетенций:

ПК 1.1.: Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.1.1: Знать состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств
ПК 1.1.2: Уметь осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем
ПК 1.1.3: Иметь практический опыт установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем

2.3	**Иметь практический опыт:**
2.3.1	ПК 1.1: Иметь навыки установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
2.3.2	ПК 1.2: Иметь навыки администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении.
2.3.3	ПК 1.3: Иметь навыки обеспечения бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
2.3.4	ПК 1.4: Иметь навыки и опыт деятельности по проверке технического состояния, техническому обслуживанию, текущему ремонту, устранению отказов и восстановлению работоспособности автоматизированных (информационных) систем в защищенном исполнении.

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 АРХИТЕКТУРЫ И ПРИНЦИПОВ РАБОТЫ ОПЕРАЦИОННЫХ СИСТЕМ				
1. 1	Тема 1.1. Эволюция, классификация и общие принципы построения операционных систем Исторические этапы развития ОС. Основные понятия (ядро, драйверы, интерфейсы). Классификация ОС по назначению, способу управления ресурсами, типу архитектуры (монолитная, микроядерная, гибридная). Функции ОС по управлению процессами, памятью, файловой системой и вводом-выводом. Знать: определение операционной системы и её основные функции; классификацию ОС по различным признакам; этапы эволюции ОС; различия между монолитным и микроядерным ядром; основные компоненты ОС (ядро, оболочка, утилиты); понятие системного вызова; принципы работы с аппаратурой на уровне ОС; базовые модели управления ресурсами; назначение драйверов устройств; критерии выбора ОС для автоматизированных систем. /Лек/	3	4/0	ПК 1.1.1	Устный опрос
1. 2	Лабораторная работа № 1. Установка и базовая	3	4/0	ПК	Отчет по лабораторной

	настройка операционной системы в защищенном исполнении. Уметь: устанавливать ОС с заданными параметрами безопасности; настраивать базовые политики учетных записей; конфигурировать параметры ядра для обеспечения минимального атакующего воздействия. Владеть: навыками работы с инсталлятором ОС; навыками настройки прав доступа к файлам и каталогам; навыками проверки целостности системных файлов. /Лаб/			1.1.2,ПК 1.1.3	работе
1. 3	Самостоятельная работа по теме «Сравнительный анализ архитектур ОС семейства Windows и Linux с точки зрения защищенности». /СР/	3	2/0	ПК 1.1.1,ПК 1.1.2,ПК 1.1.3	Вопросы для самоподготовки
1. 4	Тема 1.2. Управление процессами и потоками Модели процессов и потоков. Состояния процесса. Контекст переключения. Алгоритмы планирования (FCFS, SJF, RR, приоритетное). Синхронизация процессов (мьютексы, семафоры, мониторы). Тупики и методы их предотвращения. Знать: определение процесса и потока; диаграмму состояний процесса; структуру контекста процесса; основные алгоритмы планирования; цели и средства синхронизации; определение взаимной блокировки; условия возникновения тупиков (Коффмана); методы обнаружения и предотвращения тупиков; понятие приоритетов и инверсии приоритетов; роль диспетчера процессов. /Лек/	3	4/0	ПК 1.1.1	Устный опрос
1. 5	Лабораторная работа № 2. Исследование планировщиков процессов в ОС. Уметь: изменять приоритеты процессов в реальном времени; анализировать загрузку процессора при разных алгоритмах планирования; интерпретировать вывод системных утилит (top, ps, task manager). Владеть: навыками запуска и остановки процессов; навыками мониторинга состояния процессов; навыками настройки параметров планирования через системные вызовы. /Лаб/	3	4/0	ПК 1.1.2,ПК 1.1.3	Отчет по лабораторной работе
1. 6	Тема 1.3. Управление памятью и виртуальная память Схемы организации памяти (непрерывное распределение, сегментация, страничная организация). Механизмы трансляции адресов. Алгоритмы замещения страниц (FIFO, LRU, Second Chance). Подкачка. Страничные ошибки. Защита памяти. Знать: виды адресов (логический, физический, линейный); принципы сегментации и страничного распределения; структуру таблицы страниц; алгоритмы замещения страниц и их сравнительные характеристики; понятие TLB (буфер ассоциативной трансляции); механизм подкачки; причины возникновения страничных ошибок; способы защиты памяти; преимущества виртуальной памяти; влияние настроек подкачки на производительность АС. /Лек/	3	4/0	ПК 1.1.1	Устный опрос
1. 7	Лабораторная работа № 3. Настройка параметров виртуальной памяти и мониторинг подкачки. Уметь: изменять размер файла подкачки;	3	4/0	ПК 1.1.2,ПК 1.1.3	Отчет по лабораторной работе

	настраивать параметры кэширования страниц; диагностировать интенсивность страничных обменов. Владеть: навыками работы с утилитами мониторинга памяти; навыками настройки параметров ядра, влияющих на VM; навыками интерпретации логов страничных ошибок. /Лаб/				
	2. РАЗДЕЛ 2. ФАЙЛОВЫЕ СИСТЕМЫ И УСТРОЙСТВА ВВОДА-ВЫВОДА				
2. 1	Тема 2.1. Организация файловых систем и управление данными Логическая структура файловых систем (FAT, NTFS, ext4, XFS. Методы распределения дискового пространства. Журналирование. ,Управление разрешениями (ACL, атрибуты). Монтирование. Целостность данных. Шифрование файловых систем. Знать: структуру суперблока, индексных дескрипторов, таблиц FAT; различия между журналируемыми и нежурналируемыми ФС; механизмы разграничения доступа на основе прав и ACL; принципы работы с жесткими и символическими ссылками; этапы монтирования ФС; методы восстановления поврежденной ФС; влияние ФС на производительность АС; возможности шифрования на уровне ФС; понятие квот и их настройку; совместимость ФС с разными ОС в защищенном исполнении. /Лек/	3	6/0	ПК 1.1.1	Устный опрос
2. 2	Лабораторная работа № 4. Настройка прав доступа, квот и шифрования в файловой системе. Уметь: создавать и изменять ACL для пользователей и групп; устанавливать квоты на дисковое пространство; настраивать шифрование отдельных каталогов (LUKS, EFS). Владеть: навыками работы с командами chmod, setfacl, quotacheck; навыками монтирования зашифрованных разделов; навыками проверки целостности ФС с помощью встроенных средств. /Лаб/	3	6/0	ПК 1.1.2,ПК 1.1.3	Отчет по лабораторной работе
2. 3	Тема 2.2. Управление устройствами ввода-вывода и драйверами Архитектура подсистемы ввода-вывода Типы устройств (символьные, блочные, сетевые). Интерфейсы драйверов. Механизмы прерываний и DMA. Буферизация. Кэширование. Очереди запросов. Управление электропитанием устройств. Знать: различие между блочными и символьными устройствами; роль драйвера в ОС; принцип работы прерываний и обработчиков прерываний; механизм прямого доступа к памяти (DMA); структуру буферного кэша; алгоритмы планирования запросов к диску (NOOP, CFQ, Deadline); способы загрузки и выгрузки драйверов; настройки тайм-аутов для устройств; влияние драйверов на безопасность АС; методы отладки драйверов. /Лек/	3	6/0	ПК 1.1.1	Устный опрос
2. 4	Лабораторная работа № 5. Установка и настройка драйверов периферийных устройств в защищенной АС. Уметь: идентифицировать оборудование; загружать, выгружать и перекомпилировать драйверы (в модульном ядре); настраивать параметры драйвера через системные файлы.	3	6/0	ПК 1.1.2,ПК 1.1.3	Отчет по лабораторной работе

	Владеть: навыками сборки модулей ядра; навыками настройки параметров устройств через sysfs; навыками тестирования работоспособности устройств после изменения конфигурации. /Лаб/				
	3. РАЗДЕЛ 3. СЕТИ, РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ И КОМПОНЕНТЫ ЗАЩИТЫ ИНФОРМАЦИИ				
3. 1	Тема 3.1. Сетевые подсистемы ОС и стеки протоколов Сетевые интерфейсы ОС. Реализация стека TCP/IP, маршрутизация. Настройка межсетевого экрана (iptables/nftables, Windows Firewall). Сетевые службы (DHCP, DNS). Удаленное управление (SSH, RDP). VLAN, VPN. Знать: структуру сетевого стека в ОС; способы настройки IP-адресации и маршрутов; принципы фильтрации пакетов; различия между stateful и stateless firewall; протоколы удаленного доступа и их уязвимости; настройку сетевых мостов и агрегации каналов; методы диагностики сети (ping, traceroute, netstat); параметры безопасности сетевых служб; принципы работы VLAN в ОС; основы настройки VPN-клиентов и серверов. /Лек/	3	6/0	ПК 1.1.1	Устный опрос
3. 2	Лабораторная работа № 6. Конфигурирование сетевого экрана и фильтрация трафика. Уметь: создавать правила фильтрации входящего/исходящего трафика; настраивать NAT и порт-форвардинг; организовывать защищенный канал (SSH-туннель). Владеть: навыками работы с iptables/nftables; навыками проверки активных соединений; навыками логирования сетевых событий. /Лаб/	3	6/0	ПК 1.1.2,ПК 1.1.3	Отчет по лабораторной работе
3. 3	Тема 3.2. Основы защиты информации в ОС. Политики безопасности, аудит и шифрование Мандатное и дискреционное управление доступом. Средства аудита (syslog, auditd). Настройка политик паролей. Шифрование дисков и каналов связи. Защита от вредоносного кода. Изоляция процессов (контейнеры, песочницы). Аттестация ОС по требованиям защищенных систем. Знать: различия между DAC, MAC и RBAC; настройку системного аудита (журналы, алерты); механизмы шифрования на лету; требования к парольной политике; методы обнаружения вторжений на уровне ОС; принципы работы контейнерной изоляции; настройку SELinux/AppArmor; порядок аудита событий безопасности; критерии оценки защищенности ОС; основы аттестации АС в защищенном исполнении. /Лек/	3	6/0	ПК 1.1.1	Устный опрос
3. 4	Лабораторная работа № 7. Настройка политик безопасности, аудита и мандатного контроля доступа. Уметь: включать и настраивать SELinux/AppArmor; настраивать auditd для отслеживания критичных файлов; применять политики паролей и блокировки учетных записей. Владеть: навыками работы с утилитами аудита; навыками восстановления доступа при сбоях политик; навыками документирования настроек безопасности.	3	6/2	ПК 1.1.2,ПК 1.1.3	Отчет по лабораторной работе

	/Лаб/				
3. 5	Самостоятельная работа по теме «Сравнительный анализ мандатных и дискреционных политик доступа на примере SELinux и стандартных прав UNIX». /СР/	3	2/0	ПК 1.1.1,ПК 1.1.2,ПК 1.1.3	Вопросы для самоподготовки
	4. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ				
4. 1	Контрольная работа ПК 1.1.1 Знать состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств ПК 1.1.2 Уметь осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем ПК 1.1.3 Иметь практический опыт установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем /СР/	3	0/0	ПК 1.1.1,ПК 1.1.2,ПК 1.1.3	Вопросы для контрольной работы, итоговое тестирование
	5. РАЗДЕЛ 4. АДМИНИСТРИРОВАНИЕ, ОПТИМИЗАЦИЯ И ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ				
5. 1	Тема 4.1. Инструменты мониторинга, резервного копирования и восстановления Системные утилиты мониторинга (top, htop, iostat, vmstat). Средства резервного копирования (rsync, tar, dd). Планировщики заданий (cron, systemd timers). Стратегии бэкапа (полный, инкрементный, дифференциальный). Восстановление системы после сбоев. Создание Live-образов. Знать: ключевые метрики производительности ОС; методы сбора статистики; форматы резервных копий; настройку периодических заданий; способы восстановления загрузчика и поврежденных файлов; принципы создания загрузочных носителей; утилиты проверки целостности файлов; логирование ошибок; стратегии архивации с сжатием; планирование времени обслуживания для минимизации простоя АС. /Лек/	3	6/0	ПК 1.1.1	Устный опрос
5. 2	Лабораторная работа № 8. Настройка мониторинга и автоматического резервного копирования. Уметь: настраивать сбор метрик в реальном времени; создавать скрипты для инкрементного бэкапа; планировать задания через cron с уведомлениями об ошибках. Владеть: навыками работы с архиваторами и инструментами синхронизации; навыками восстановления файлов из бэкапа; навыками настройки ротации логов. /Лаб/	3	6/0	ПК 1.1.2,ПК 1.1.3	Отчет по лабораторной работе
5. 3	Тема 4.2. Практические аспекты установки, настройки и аттестации защищенных АС Обобщаются знания по комплектованию АС, выбору компонентов ОС с учетом требований защищенности, порядку настройки всех подсистем (память, ФС, сеть, аудит), документированию конфигурации, тестированию	3	6/0	ПК 1.1.1	Устный опрос

	на уязвимости, подготовке к аттестации. Знать: этапы жизненного цикла защищенной АС; перечень обязательных мероприятий при развертывании; типовые схемы конфигураций для разных классов защищенности; методы тестирования защищенности (сканирование портов, анализ журналов); требования к документации на АС; роли администраторов и пользователей; порядок обновлений и патчей; процедуру проверки целостности ПО; критерии выбора аппаратной платформы; основы проведения аттестационных испытаний. /Лек/				
5. 4	Лабораторная работа № 9. Комплексная настройка автоматизированной системы в защищенном исполнении. Уметь: выполнять полную установку ОС с параметрами безопасности (зашифрованный раздел, минимальный набор служб, настроенный firewall, аудит); проводить проверку соответствия политике безопасности; составлять отчет о настройке. Владеть: навыками интеграции всех компонентов СЗИ; навыками документирования конфигурации; навыками проведения базового тестирования на проникновение (пентест) на уровне ОС. /Лаб/	3	6/2	ПК 1.1.2,ПК 1.1.3	Отчет по лабораторной работе

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

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ

Оценочные средства текущего контроля успеваемости:

ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1.1. Эволюция, классификация и общие принципы построения ОС
1. Что такое операционная система и какие основные функции она выполняет?
2. По каким критериям классифицируют современные ОС?
3. Назовите основные этапы исторического развития ОС.
4. Чем монолитное ядро отличается от микроядра?
5. Какие компоненты входят в состав ядра ОС?
6. Что такое системный вызов и как он реализуется?
7. Как происходит взаимодействие драйверов с аппаратным обеспечением?
8. Какие модели управления ресурсами используются в ОС?
9. Перечислите критерии выбора ОС для защищенной автоматизированной системы.
10. Какие интерфейсы (пользовательские и программные) предоставляет ОС?

Тема 1.2. Управление процессами и потоками
1. Дайте определение процесса и потока. В чем их различия?
2. Опишите диаграмму состояний процесса.
3. Какие алгоритмы планирования процессов вы знаете?
4. Что такое контекст процесса и когда происходит его переключение?
5. Для чего нужна синхронизация процессов? Назовите основные средства.
6. Что такое взаимная блокировка (deadlock) и при каких условиях она возникает?

7. Какие методы предотвращения тупиков существуют?
8. Что такое инверсия приоритетов и как с ней борются?
9. Как работает диспетчер процессов в ОС?
10. В чем различие между вытесняющим и невытесняющим планированием?

Тема 1.3. Управление памятью и виртуальная память
1. Какие виды адресов используются в ОС и как они соотносятся?
2. В чем суть страничной организации памяти?
3. Чем сегментация отличается от страничного распределения?
4. Опишите алгоритмы замещения страниц (FIFO, LRU, Second Chance).
5. Что такое TLB и как он ускоряет трансляцию адресов?
6. Как работает механизм подкачки (swapping)?
7. Что такое страничная ошибка (page fault) и как она обрабатывается?
8. Какие способы защиты памяти реализованы в ОС?
9. В чем преимущества виртуальной памяти перед физической?
10. Как настройки виртуальной памяти влияют на производительность АС?

Тема 2.1. Организация файловых систем и управление данными
1. Перечислите основные структуры данных в файловых системах (суперблок, inode, FAT).
2. Чем журналируемые ФС отличаются от нежурналируемых?
3. Какие механизмы разграничения доступа (ACL, атрибуты) вы знаете?
4. Как происходит монтирование файловой системы?
5. Что такое жесткая и символическая ссылки?
6. Какие методы восстановления поврежденной ФС применяются?
7. Как настраиваются дисковые квоты?
8. Какие ФС поддерживают шифрование на уровне каталогов?
9. Как влияет выбор ФС на безопасность и производительность?
10. Какие особенности совместимости ФС между ОС семейства Windows и Linux?

Тема 2.2. Управление устройствами ввода-вывода и драйверами
1. В чем различие между блочными и символьными устройствами?
2. Какова роль драйвера в системе?
3. Объясните механизм аппаратных прерываний.
4. Что такое DMA и для чего он используется?
5. Как организован буферный кэш в ОС?
6. Назовите алгоритмы планирования запросов к диску.
7. Как загрузить и выгрузить драйвер в ядро?
8. Какие параметры драйверов можно настраивать для обеспечения безопасности?
9. Как отлаживать драйверы устройств?
10. Какие риски безопасности связаны с некорректными драйверами?

Тема 3.1. Сетевые подсистемы ОС и стеки протоколов
1. Как реализован стек TCP/IP в ОС?
2. Как настраиваются IP-адреса и маршруты в ОС?
3. Какие правила фильтрации трафика устанавливаются в межсетевом экране?
4. В чем различие между stateful и stateless firewall?
5. Какие протоколы удаленного управления используются и как они защищаются?
6. Для чего применяются VLAN и как они настраиваются в ОС?
7. Какие утилиты используются для диагностики сети?
8. Как настраиваются сетевые службы (DHCP, DNS) с точки зрения безопасности?
9. Какие параметры VPN влияют на защищенность канала?
10. Как агрегировать сетевые интерфейсы (bonding/teamig)?

Тема 3.2. Основы защиты информации в ОС
1. Чем отличаются дискреционное, мандатное и ролевое управление доступом?
2. Как настраивается системный аудит (auditd, syslog)?
3. Какие алгоритмы шифрования используются для шифрования дисков?
4. Требования к парольной политике в защищенных АС.
5. Как работают контейнеры и изоляция процессов (namespaces, cgroups)?
6. Что такое SELinux и AppArmor, как их настроить?
7. Какие события должны фиксироваться в журналах безопасности?
8. Как производится обнаружение вторжений на уровне ОС?
9. Назовите критерии оценки защищенности ОС.
10. Какие этапы включает аттестация АС в защищенном исполнении?

Тема 4.1. Мониторинг, резервное копирование и восстановление
1. Какие системные утилиты позволяют отслеживать загрузку процессора и памяти?
2. Что такое инкрементный и дифференциальный бэкап, их плюсы и минусы?

3. Как настроить планировщик заданий cron для автоматического бэкапа?
4. Какие средства позволяют создавать Live-образы для восстановления?
5. Как проверить целостность важных системных файлов?
6. В чем разница между утилитами rsync, tar и dd?
7. Какие метрики необходимо мониторить для предотвращения сбоев?
8. Как организовать ротацию логов и архивов?
9. Какие действия выполняются при восстановлении загрузчика ОС?
10. Как составить стратегию резервного копирования для АС с непрерывной работой?

Тема 4.2. Практическая установка, настройка и аттестация защищенных АС
1. Перечислите этапы развертывания защищенной АС.
2. Какие компоненты ОС конфигурируются в первую очередь для обеспечения безопасности?
3. Как тестируется защищенность после настройки?
4. Какие документы должны быть подготовлены для аттестации?
5. Как распределяются роли администраторов и пользователей в защищенной системе?
6. Как организовать процесс обновления и патчевания без снижения защиты?
7. Как выбрать аппаратную платформу под требования ОС?
8. Какие уязвимости наиболее характерны для неправильно настроенной ОС?
9. Что входит в проверку целостности ПО при аттестации?
10. Как проводится анализ журналов аудита для подтверждения соответствия?

ВОПРОСЫ ДЛЯ САМОПОДГОТОВКИ

Самостоятельная работа по теме «Сравнительный анализ архитектур ОС Windows и Linux с точки зрения защищенности»
1. Какие различия в модели безопасности ядра Windows и Linux?
2. Как реализовано управление доступом в Windows (UAC) и в Linux (sudo/SUID)?
3. Какие механизмы аудита предлагаются в каждой системе?
4. Какая ОС предоставляет более гибкие средства мандатного контроля?
5. Как различаются подходы к управлению пакетами и обновлениями?
6. Какая файловая система в каждой ОС обеспечивает лучшую защиту от повреждений?
7. Как организована изоляция приложений (песочницы) в Windows и Linux?
8. Какие встроенные средства шифрования доступны в обеих ОС?
9. Как различаются подходы к настройке межсетевого экрана?
10. Какие особенности лицензирования и поддержки влияют на выбор ОС для защищенной АС?

Самостоятельная работа по теме «Сравнение мандатных и дискреционных политик доступа на примере SELinux и стандартных прав UNIX»
1. В чем принципиальное отличие прав UNIX (rwx) от контекстов SELinux?
2. Как типовая политика SELinux ограничивает процессы?
3. Какие роли и типы используются в SELinux?
4. Какие преимущества дает мандатное управление доступом по сравнению с дискреционным?
5. Как переключить SELinux в режим permissive и для чего это нужно?
6. Как аудировать нарушения политики SELinux?
7. Какие ограничения есть у дискреционных прав UNIX в многопользовательской среде?
8. Как создать собственный модуль политики SELinux?
9. Как стандартные права UNIX сочетаются с расширенными атрибутами?
10. Какие сценарии требуют обязательного применения мандатного контроля в АС?

ЗАДАНИЯ НА ЛАБОРАТОРНЫЕ РАБОТЫ

РАЗДЕЛ 1. ОСНОВЫ АРХИТЕКТУРЫ И ПРИНЦИПОВ РАБОТЫ ОПЕРАЦИОННЫХ СИСТЕМ

Лабораторная работа № 1. Установка и базовая настройка операционной системы в защищенном исполнении
Задания:
1. Выполните чистую установку операционной системы Windows (или Linux) на виртуальную машину, задав параметры безопасности: использование зашифрованного раздела диска (BitLocker / LUKS) и создание отдельного раздела для системных и пользовательских данных.
2. В процессе установки создайте учетную запись администратора с надежным паролем (не менее 12 символов, включая цифры, буквы разного регистра и спецсимволы) и одну стандартную учетную запись пользователя без прав администратора.
3. После установки настройте базовые политики учетных записей через оснастку «Локальные политики безопасности» (secpol.msc): установите максимальный срок действия пароля 30 дней, минимальную длину пароля 10 символов и включите требование сложности пароля.
4. Настройте параметры ядра (для Windows – параметры реестра и загрузчика, для Linux – параметры загрузчика GRUB) для уменьшения поверхности атаки: отключите неиспользуемые службы и порты, запретите автоматическое воспроизведение внешних носителей.
5. Проверьте целостность системных файлов с помощью встроенных средств: для Windows – выполните команду

sfc /scannow, для Linux – проверьте контрольные суммы критичных файлов через пакетный менеджер.
6. Настройте права доступа к системным каталогам (например, C:\Windows\System32 или /etc), ограничив запись для стандартных пользователей, и проверьте применение прав через проверку доступа к защищенному файлу.

Лабораторная работа № 2. Исследование планировщиков процессов в ОС
Задания:
1. Запустите несколько ресурсоемких процессов (например, архивацию большого каталога, выполнение математических вычислений в PowerShell или запуск нескольких экземпляров утилиты stress для Linux). С помощью диспетчера задач Windows (или утилиты top / ps в Linux) определите их PID, приоритет и текущее состояние.
2. Измените приоритет одного из запущенных процессов в реальном времени (в Windows – через диспетчер задач, вкладка «Подробности», установите приоритет «Высокий»; в Linux – командой renice). Зафиксируйте изменения в загрузке процессора до и после изменения.
3. Запустите несколько процессов с одинаковым приоритетом и наблюдайте за распределением процессорного времени в течение 2–3 минут. Сделайте вывод о том, какой алгоритм планирования используется по умолчанию в вашей системе.
4. С помощью системных утилит (PowerShell Get-Process или Linux ps -eo pid,pri,ni,cmd) проанализируйте текущие приоритеты всех процессов и определите, какие из них имеют наивысший и наинизший приоритет.
5. Искусственно создайте ситуацию высокой загрузки процессора (запустите несколько вычислительных задач в циклах) и с помощью диспетчера задач или утилиты top отследите, как планировщик распределяет время между процессами. Опишите наблюдаемое поведение.
6. Настройте параметры планирования через системные вызовы (в Windows – использование WinAPI или PowerShell с WMI, в Linux – команда chrt для изменения политики планирования реального времени) для одного из процессов и проверьте изменение его поведения.

Лабораторная работа № 3. Настройка параметров виртуальной памяти и мониторинг подкачки
Задания:
1. Определите текущий размер файла подкачки в вашей системе (Windows: «Свойства системы» – «Дополнительно» – «Быстродействие» – «Дополнительно» – «Виртуальная память»; Linux: команда swapon --show). Запишите начальные значения.
2. Измените размер файла подкачки, увеличив его на 2048 МБ, и перезагрузите систему (или выполните перезапуск службы подкачки без перезагрузки, если это поддерживается). Проверьте, что новый размер применился.
3. Настройте параметры кэширования страниц: в Windows измените размер системного кэша через реестр (параметры LargeSystemCache), в Linux измените параметры vm.swappiness и vm.vfs_cache_pressure через sysctl. Зафиксируйте новые значения.
4. Запустите приложение, интенсивно использующее память (например, браузер с множеством вкладок или виртуальную машину) и с помощью счетчиков производительности (Windows: диспетчер задач или Performance Monitor; Linux: vmstat и /proc/meminfo) зафиксируйте количество страничных ошибок и интенсивность операций подкачки до и после изменения параметров.
5. Сымитируйте нехватку оперативной памяти, запустив несколько тяжелых приложений, и с помощью системных логов (Windows: журнал событий, Linux: dmesg или /var/log/syslog) найдите записи о страничных ошибках и действиях подсистемы виртуальной памяти.
6. Проанализируйте полученные логи и ответьте на вопрос: какие процессы вызывают наибольшее число страничных обменов. Предложите способ снижения интенсивности подкачки без увеличения физической памяти (например, закрытие неиспользуемых приложений или изменение приоритетов).

РАЗДЕЛ 2. ФАЙЛОВЫЕ СИСТЕМЫ И УСТРОЙСТВА ВВОДА-ВЫВОДА

Лабораторная работа № 4. Настройка прав доступа, квот и шифрования в файловой системе
Задания:
1. Создайте два каталога на системном диске: «Общие_данные» и «Конфиденциально». Настройте для каталога «Конфиденциально» следующие права через оснастку «Безопасность» (или команду icacls в Windows / setfacl в Linux): доступ на чтение и запись только для администратора, доступ на чтение для группы «Пользователи», доступ запрещен для всех остальных.
2. Для каталога «Общие_данные» создайте список ACL, разрешающий пользователю «user1» полный доступ, пользователю «user2» доступ только на чтение, а группе «Пользователи» – доступ на запись и чтение. Проверьте применение прав, войдя в систему под разными учетными записями.
3. Установите дисковые квоты для раздела данных: ограничьте каждого пользователя 1 ГБ дискового пространства с предупреждением при достижении 800 МБ. Проверьте работу квот, скопировав в каталог пользователя файлы большего размера.
4. Настройте шифрование каталога «Конфиденциально» с помощью встроенных средств Windows (EFS – свойства папки, «Дополнительно», шифрование содержимого) или Linux (создание зашифрованного каталога через ecryptfs или LUKS-раздел). Проверьте, что файлы внутри отображаются зашифрованными для другого пользователя.
5. Выполните проверку целостности файловой системы на системном разделе с помощью встроенных утилит: в Windows – команда chkdsk /f /r (без перезагрузки, с планированием), в Linux – fsck для соответствующего раздела. Сделайте вывод о наличии ошибок.
6. Создайте нового пользователя и настройте для него автоматическое монтирование зашифрованного раздела (или каталога) при входе в систему с использованием сохраненного ключа или пароля.

Лабораторная работа № 5. Установка и настройка драйверов периферийных устройств в защищенной АС

Задания:
1. Идентифицируйте все подключенные к системе устройства с помощью диспетчера устройств Windows (или команд lspci и lsusb в Linux). Запишите идентификаторы (VID/PID) сетевой карты и звукового устройства.
2. Скачайте с официального сайта производителя актуальную версию драйвера для сетевой карты, установите его вручную (через «Обновить драйвер» или установочный пакет). Убедитесь, что устройство работает корректно.
3. Для устройства, работающего с системным драйвером (например, принтер или USB-накопитель), выгрузите текущий драйвер (в Windows – отключите устройство в диспетчере и удалите драйвер; в Linux – выполните modprobe -r для модуля) и загрузите его заново, не перезагружая систему.
4. Настройте параметры драйвера сетевой карты через системные файлы: в Windows – через свойства сетевого адаптера (отключение энергосбережения, настройка Jumbo-кадров), в Linux – через файлы в /sys/class/net/.../device/ или параметры модуля в /etc/modprobe.d/.
5. Протестируйте работоспособность устройства после изменения параметров: для сетевой карты – выполните пинг до внешнего узла и проверьте скорость передачи файла; для принтера – распечатайте тестовую страницу.
6. Соберите модуль ядра для вымышленного простого устройства (в Linux – на основе шаблона модуля «hello world»; в Windows – создайте тестовый драйвер с помощью WDK или опишите процесс сборки для заданного примера). Убедитесь, что модуль загружается и выгружается без ошибок.

РАЗДЕЛ 3. СЕТИ, РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ И КОМПОНЕНТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лабораторная работа № 6. Конфигурирование сетевого экрана и фильтрация трафика
Задания:
1. С помощью встроенного брандмауэра Windows (или iptables/nftables в Linux) создайте правило, блокирующее все входящие подключения к порту 3389 (RDP) из внешней сети, но разрешающее подключения из локальной подсети (например, 192.168.1.0/24).
2. Настройте правило для исходящего трафика, запрещающее приложениям из папки «Загрузки» устанавливать соединения с внешними IP-адресами (кроме адресов обновлений). Проверьте работу, попытавшись запустить скачанный браузер.
3. Настройте перенаправление портов (порт-форвардинг) таким образом, чтобы входящие соединения на порт 8080 перенаправлялись на локальный веб-сервер, работающий на порту 80. Проверьте доступность веб-сервера извне.
4. Организуйте защищенный канал с помощью SSH-туннеля (на Linux) или с использованием встроенного клиента SSH в Windows 10/11: настройте проброс локального порта на удаленный сервер и проверьте передачу данных.
5. Включите логирование сетевых событий (отклоненные и разрешенные подключения) и проанализируйте журнал брандмауэра, найдя записи о блокировке тестового подключения на запрещенный порт.
6. Создайте правило динамической блокировки: при обнаружении 5 неудачных попыток подключения на порт SSH (22) за 1 минуту блокируйте IP-адрес отправителя на 10 минут (с использованием iptables + fail2ban или аналогичного инструмента в Windows через задачи планировщика).

Лабораторная работа № 7. Настройка политик безопасности, аудита и мандатного контроля доступа
Задания:
1. Включите и настройте систему мандатного контроля доступа: в Windows – через оснастку «Локальные политики безопасности» настройте параметры аудита и политики проверки подлинности; в Linux – переключите SELinux в режим enforcing и проверьте его статус командой getenforce.
2. Настройте auditd (Windows – «Политика аудита» в разделе «Конфигурация компьютера») для отслеживания следующих событий: неудачные попытки входа в систему, изменение прав доступа к файлу C:\Secret\data.txt (или /etc/shadow), запуск командной оболочки (cmd / bash).
3. Примените политику паролей: установите минимальную длину пароля 12 символов, обязательное использование цифр и спецсимволов, срок действия пароля 45 дней, блокировку учетной записи после 3 неудачных попыток на 15 минут. Проверьте на практике, что попытка установить простой пароль отклоняется.
4. Создайте локальную политику ограничений, запрещающую запуск исполняемых файлов из каталога C:\Temp (или /tmp) для всех пользователей, кроме администратора. Проверьте, что запуск файла из этого каталога блокируется.
5. Смоделируйте сбой политики SELinux/AppArmor (измените контекст важного файла) и восстановите доступ, используя утилиту restorecon или переустановку профиля AppArmor. Для Windows – сбросьте политики через secedit /configure.
6. Составьте отчет по настройкам безопасности: запишите все примененные политики, включенные аудит-правила и параметры мандатного контроля. Отчет оформите в виде текстового документа с описанием каждого шага.

РАЗДЕЛ 4. АДМИНИСТРИРОВАНИЕ, ОПТИМИЗАЦИЯ И ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Лабораторная работа № 8. Настройка мониторинга и автоматического резервного копирования
Задания:
1. Настройте сбор метрик производительности в реальном времени с помощью системных средств: в Windows – используйте Performance Monitor (счетчики процессора, памяти, диска), в Linux – top/htop и vmstat. Настройте вывод обновляемой статистики на экран.
2. Создайте скрипт для инкрементного резервного копирования папки C:\Data (или /home/user/data) в каталог C:\Backup (или /backup). Скрипт должен копировать только те файлы, которые изменились с момента последнего копирования (в Windows – используйте robocopy с ключом /MIR, в Linux – rsync -a --link-dest).
3. Настройте автоматическое выполнение этого скрипта ежедневно в 23:00 с помощью планировщика задач Windows (или cron в Linux). Добавьте уведомление об ошибке в системный журнал.

4. Настройте ротацию логов для системного журнала (Windows – через задачу планировщика по архивации старых логов; Linux – через logrotate), чтобы логи не занимали более 500 МБ и хранились не дольше 7 дней.
5. Выполните восстановление отдельных файлов из созданной резервной копии (инкрементной) в альтернативную папку. Проверьте, что восстановленные файлы идентичны оригинальным.
6. Настройте дополнительное задание для полного резервного копирования раздела системы в образ (с использованием wbadmin в Windows или dd / partimage в Linux) с запуском по воскресеньям в 02:00. Проверьте создание образа.

Лабораторная работа № 9. Комплексная настройка автоматизированной системы в защищенном исполнении
Задания:
1. Выполните полную чистую установку ОС Windows (или Linux) на виртуальную машину с параметрами безопасности: зашифрованный системный раздел (BitLocker / LUKS), отдельный раздел для данных, установка минимального набора служб (отключены все неиспользуемые роли и компоненты).
2. Настройте межсетевой экран: разрешите только исходящие соединения для обновлений (HTTP/HTTPS) и входящие – только для административного доступа (RDP или SSH из доверенной подсети). Все остальные порты заблокируйте.
3. Включите аудит всех критических событий: вход/выход, изменение прав, запуск служб, ошибки безопасности. Настройте отправку тревожных сообщений в системный журнал при обнаружении 3 неудачных входов подряд.
4. Проведите проверку соответствия настроек политике безопасности организации (из предложенного шаблона): сравните примененные параметры с эталонным списком и отметьте отклонения.
5. Составьте отчет о выполненной настройке в виде документа, содержащего: версию ОС, список установленных обновлений, примененные правила брандмауэра, параметры аудита, политики паролей, статус шифрования.
6. Выполните базовое тестирование на проникновение на уровне ОС: попытайтесь получить доступ к защищенному файлу из-под стандартной учетной записи, выполните сканирование открытых портов с внутреннего хоста и проверьте, реагирует ли система на попытки подбора пароля (блокировка учетной записи). Зафиксируйте результаты.
7. Проанализируйте журналы аудита после тестирования, найдите записи о попытках несанкционированного доступа и предложите дополнительные меры защиты, если тесты показали уязвимости.

Оценочные средства промежуточной аттестации:

ВОПРОСЫ К КОНТРОЛЬНОЙ РАБОТЕ:

Индикатор ЗНАТЬ

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

1. Установите правильную последовательность этапов обработки прерывания в операционной системе.
А) Определение источника прерывания
Б) Сохранение контекста текущего процесса
В) Передача управления обработчику прерывания
Г) Восстановление контекста и продолжение выполнения
2. Установите правильную последовательность действий при страничном обращении к памяти (при отсутствии страницы в оперативной памяти).
А) Генерация страничной ошибки (page fault)
Б) Загрузка требуемой страницы с диска в оперативную память
В) Обращение к виртуальному адресу со стороны процесса
Г) Обновление таблицы страниц и возобновление выполнения инструкции
3. Установите правильную последовательность инициализации аппаратных устройств при загрузке операционной системы.
А) Загрузка драйверов шины (PCI, USB)
Б) Обнаружение и идентификация подключенных устройств
В) Загрузка драйвера конкретного устройства
Г) Инициализация регистров устройства и выделение ресурсов (прерывания, порты)
4. Установите правильную последовательность действий при создании нового процесса в ОС.
А) Выделение памяти под образ процесса и структуры данных ядра
Б) Загрузка кода и данных исполняемого файла в выделенную память
В) Инициализация контекста процесса (регистры, стек, счетчик команд)
Г) Помещение процесса в очередь готовых к выполнению
5. Установите правильную последовательность операций при монтировании файловой системы в Linux.
А) Проверка целостности суперблока и журнала (при необходимости)
Б) Создание точки монтирования (каталога)
В) Чтение суперблока файловой системы
Г) Присоединение корневого каталога ФС к точке монтирования
6. Установите правильную последовательность обработки сетевого пакета при прохождении через межсетевой экран (firewall) в ОС.
А) Проверка состояния соединения (stateful inspection)
Б) Применение правил фильтрации по заголовкам пакета
В) Прием пакета сетевой картой и передача в стек ядра
Г) Разрешение или блокировка пакета на основе всех проверок
7. Установите правильную последовательность действий администратора при аттестации автоматизированной системы

в защищенном исполнении.
А) Документирование текущей конфигурации ОС и СЗИ
Б) Проведение тестов на уязвимости и анализ журналов аудита
В) Определение перечня защищаемых ресурсов и модели угроз
Г) Подготовка заключения о соответствии системы требованиям безопасности
8. Установите соответствие между типом операционной системы и её характерной особенностью.
А) Монолитная ОС
Б) Микроядерная ОС
В) Гибридная ОС
Г) Модульная ОС
1. Большинство драйверов работают в пространстве пользователя
2. Сочетает монолитное ядро с возможностью динамической загрузки модулей
3. Все компоненты ядра работают в едином адресном пространстве
4. Ядро небольшого размера, основные службы вынесены в пользовательский режим
5. Используется в большинстве современных дистрибутивов Linux
9. Установите соответствие между алгоритмом планирования процессов и его основным принципом.
А) FCFS (First-Come, First-Served)
Б) SJF (Shortest Job First)
В) Round Robin (RR)
Г) Приоритетное планирование
1. Каждый процесс получает квант времени по очереди
2. Выполняется процесс с наивысшим приоритетом, низкие могут ждать бесконечно
3. Первым выполняется процесс, поступивший первым
4. Выбирается процесс с наименьшим оставшимся временем выполнения
5. Используется для пакетной обработки без интерактивности
10. Установите соответствие между алгоритмом замещения страниц и его описанием.
А) FIFO
Б) LRU
В) Second Chance (алгоритм часов)
Г) Оптимальный алгоритм (Belady)
1. Заменяется страница, которая дольше всех не использовалась
2. Заменяется самая старая по времени загрузки страница
3. Заменяется страница, которая не будет использоваться дольше всех в будущем (теоретический)
4. Страница получает второй шанс, если на нее был бит обращения
5. Использует счетчик обращений к странице за последний интервал времени
11. Установите соответствие между типом файловой системы и её ключевой характеристикой.
А) FAT32
Б) NTFS
В) ext4
Г) ZFS
1. Журналирование метаданных, поддержка расширенных атрибутов и ACL
2. Простота, совместимость с разными ОС, ограничение на размер файла 4 ГБ
3. Поддержка снапшотов, пулов хранения и высокой отказоустойчивости
4. Отсутствие журналирования, ограниченная защита от сбоев
5. Используется в основном во встраиваемых системах
12. Установите соответствие между средством защиты информации в ОС и его функцией.
А) SELinux
Б) Аудит (auditd)
В) Межсетевой экран (iptables)
Г) Шифрование диска (LUKS)
1. Регистрация событий безопасности в журналах
2. Реализация мандатного управления доступом на основе политик
3. Фильтрация сетевых пакетов по правилам
4. Шифрование данных на уровне блочного устройства
5. Обнаружение вторжений в реальном времени
13. Установите соответствие между утилитой мониторинга и отслеживаемым параметром.
А) top (htop)
Б) iostat
В) vmstat
Г) netstat
1. Статистика по сетевым соединениям и маршрутам
2. Информация о загрузке процессора, памяти и процессах в реальном времени
3. Статистика операций ввода-вывода на дисковых устройствах
4. Сводная информация о подкачке, прерываниях и контекстных переключениях
5. Использование графического процессора
14. Установите соответствие между компонентом системы управления памятью и его назначением.
А) TLB (Translation Lookaside Buffer)
Б) Таблица страниц

В) Файл подкачки (swap)
Г) Алгоритм LRU
1. Хранит отображения виртуальных адресов на физические для всех процессов
2. Кэш для быстрой трансляции адресов, уменьшающий количество обращений к таблице страниц
3. Используется для выбора страниц на выгрузку при нехватке оперативной памяти
4. Механизм выбора страницы для замещения, основанный на давности использования
5. Определяет размер страницы в системе
15. Установите соответствие между этапом жизненного цикла защищенной АС и выполняемым действием.
А) Проектирование
Б) Развертывание и настройка
В) Эксплуатация и мониторинг
Г) Аттестация
1. Анализ журналов событий и реагирование на инциденты
2. Формирование модели угроз и выбор политик безопасности
3. Проверка соответствия системы утвержденным требованиям и оформление заключения
4. Установка ОС, драйверов, СЗИ и применение настроек безопасности
5. Разработка интерфейсов для конечных пользователей

Индикатор УМЕТЬ

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

1. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Какая архитектура операционной системы обеспечивает наивысшую отказоустойчивость за счет того, что большинство сервисов работают в отдельных адресных пространствах и могут перезапускаться без перезагрузки всего ядра?
А) Монолитная архитектура
Б) Микроядерная архитектура
В) Гибридная архитектура
Г) Модульная архитектура с монолитным ядром
2. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Какой алгоритм планирования процессов гарантирует, что ни один процесс не будет испытывать «голодание» (starvation) при условии корректного выбора кванта времени?
А) First-Come, First-Served (FCFS)
Б) Shortest Job First (SJF)
В) Round Robin (RR)
Г) Приоритетное планирование без вытеснения
3. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При возникновении страничной ошибки (page fault) операционная система сначала пытается найти свободный кадр памяти. Если свободных кадров нет, то применяется алгоритм замещения. Какой из перечисленных алгоритмов гарантирует минимальное количество страничных ошибок на практике (при известных данных о будущих обращениях, но недоступных системе)?
А) FIFO (First In, First Out)
Б) LRU (Least Recently Used)
В) Оптимальный алгоритм (Belady)
Г) Second Chance (алгоритм часов)
4. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Для автоматизированной системы, обрабатывающей конфиденциальные данные, критически важно разграничение доступа на уровне отдельных процессов и файлов, при котором права определяются не только владельцем, но и централизованной политикой, обязательной для всей системы. Какой тип управления доступом соответствует этому требованию?
А) Дискреционное управление доступом (DAC)
Б) Мандатное управление доступом (MAC)
В) Управление доступом на основе списков ACL
Г) Ролевое управление доступом (RBAC) без мандатных меток
5. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. В ходе настройки защищенной автоматизированной системы администратору необходимо обеспечить возможность восстановления данных после сбоя питания без потери уже подтвержденных транзакций файловой системы. Какая характеристика файловой системы является ключевой для решения этой задачи?
А) Поддержка разреженных файлов
Б) Наличие журналирования с режимом ordered или data=journal
В) Возможность дефрагментации онлайн
Г) Поддержка квот на дисковое пространство
6. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При проведении аудита безопасности администратор обнаруживает множество неудачных попыток входа в систему в ночное время из недоверенного сетевого сегмента. Какой компонент ОС позволит автоматически блокировать такие попытки после заданного числа неудач, не изменяя правил межсетевого экрана?
А) Система системных вызовов (syscalls)
Б) Подсистема PAM (Pluggable Authentication Modules) с модулем pam_tally2 или pam_faillock
В) Планировщик заданий cron

Г) Драйвер сетевого интерфейса
7. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При подготовке к аттестации автоматизированной системы в защищенном исполнении необходимо проверить, что все события изменения прав доступа к критичным файлам регистрируются и хранятся не менее заданного срока. Какой инструмент в ОС семейства Linux позволяет настроить такую выборочную регистрацию на уровне ядра?
А) syslog (rsyslog)
Б) systemd-journald
В) auditd с настроенными правилами (audit rules) на отслеживание конкретных файлов
Г) утилита strace для трассировки системных вызовов

Индикатор ИМЕТЬ НАВЫКИ И (ИЛИ) ОПЫТ ДЕЯТЕЛЬНОСТИ

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

1. Прочитайте текст и запишите развернутый ответ. В автоматизированной системе, работающей под управлением Linux, обнаружена уязвимость: любой пользователь может просматривать содержимое файла /etc/shadow, хотя по политике безопасности доступ к нему должен быть только у суперпользователя. Администратор проверил права командой ls -l /etc/shadow и увидел: -rw-r--r-- 1 root root. Какое действие должен предпринять администратор для устранения проблемы и почему изменение только владельца или группы здесь не поможет?
2. Прочитайте текст и запишите развернутый ответ. Серверное приложение работает с базой данных и активно использует файловую систему. В часы пик наблюдается резкое падение производительности, а утилита iostat показывает высокую загрузку диска (свыше 90%) при низком использовании процессора. Администратор предлагает увеличить объем оперативной памяти. Объясните, как увеличение ОЗУ может повлиять на дисковую загрузку в данном случае и какие параметры ОС нужно дополнительно проверить.
3. Прочитайте текст и запишите развернутый ответ. В организации внедряется новая АС, которая должна соответствовать требованиям защиты информации. Установлена ОС с поддержкой SELinux в режиме enforcing. Однако после настройки сервис не может записать данные в свой рабочий каталог, хотя права доступа UNIX (rwx) выставлены корректно. Журнал аудита показывает отказ по причине avc: denied. В чем причина ошибки и какие два способа ее решения существуют?
4. Прочитайте текст и запишите развернутый ответ. Согласно регламенту, резервное копирование баз данных должно выполняться каждый день в 2:00 ночи. Администратор настроил задание в cron, но через неделю обнаружил, что резервные копии создавались нерегулярно, а в некоторых случаях задание вообще не выполнялось. В логах указано, что команда запускалась, но завершалась с ошибкой «No space left on device». Почему задание могло выполняться не каждый день и как исправить ситуацию, не меняя основное хранилище?
5. Прочитайте текст и запишите ответ. В системе настроен файл подкачки объемом 2048 МБ. Средний размер выгружаемой страницы равен 4 КБ. Сколько максимально страниц может быть одновременно выгружено в файл подкачки, если считать, что весь файл используется только под страницы? Разрешается использовать калькулятор.
6. Прочитайте текст и запишите ответ. Планировщик использует квант времени 50 миллисекунд. В очереди готовых процессов находятся 5 процессов с одинаковым приоритетом, каждый требует 200 миллисекунд процессорного времени. Сколько полных квантов получит первый процесс до завершения, если переключение контекста занимает 5 миллисекунд и не влияет на учет времени выполнения? Разрешается использовать калькулятор.
7. Прочитайте текст и запишите ответ. Для хранения таблицы страниц используется 4 байта на одну запись. Объем виртуального адресного пространства процесса – 4 ГБ, размер страницы – 4 КБ. Сколько памяти (в МБ) требуется для хранения полной таблицы страниц одного процесса? Разрешается использовать калькулятор.
8. Прочитайте текст и запишите ответ. В системе аудита установлено ограничение на размер журнала 500 МБ. В среднем за час записывается 20 МБ событий. Через сколько часов журнал полностью заполнится, если в начале его размер составлял 100 МБ? Разрешается использовать калькулятор.

ИТОГОВОЕ ТЕСТИРОВАНИЕ

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

1. Что такое операционная система?
а) Программа для редактирования текстов
б) Интерфейс между аппаратным и программным обеспечением
в) Устройство хранения данных
г) Вид антивирусного ПО
2. Какой из перечисленных видов НЕ является типом операционной системы?
а) Пакетная
б) Интерактивная
в) Графическая
г) Реальная
3. Как называется программа, загружающая ОС?
а) Драйвер
б) BIOS
в) Загрузчик

г) Компилятор
4. Какой компонент ОС отвечает за взаимодействие с аппаратными устройствами?
а) Файловая система
б) Драйвер
в) Командный процессор
г) Кэш-память
5. Что означает аббревиатура BIOS?
а) Basic Input/Output System
б) Binary Input/Output Standard
в) Boot Initialization Operating System
г) Basic Integrated Operating Software
6. Что такое процесс в операционной системе?
а) Программа в состоянии выполнения
б) Аппаратный компонент компьютера
в) Тип файловой системы
г) Вид системного вызова
7. Какой алгоритм используется для замещения страниц в виртуальной памяти?
а) FIFO (First In, First Out)
б) LIFO (Last In, First Out)
в) RANDOM (Случайный выбор)
г) Все перечисленные
8. Что из перечисленного НЕ является типом файловой системы?
а) FAT32
б) NTFS
в) HTTP
г) ext4
9. Как называется ситуация, когда два процесса ждут ресурсы друг друга?
а) Синхронизация
б) Взаимоблокировка (Deadlock)
в) Инкапсуляция
г) Виртуализация
10. Какой механизм позволяет процессам обмениваться данными?
а) Виртуальная память
б) Межпроцессное взаимодействие (IPC)
в) Фрагментация
г) Кэширование
11. Что такое гипервизор?
а) Программа для создания виртуальных машин
б) Тип файловой системы
в) Компонент для управления памятью
г) Вид системного вызова
12. Какой тип гипервизора работает напрямую с аппаратурой?
а) Type 1 (Bare-metal)
б) Type 2 (Hosted)
в) Type 3 (Гибридный)
г) Type 4 (Сетевой)
13. Что из перечисленного НЕ является угрозой безопасности ОС?
а) Вирусы
б) DDoS-атаки
в) Кэширование данных
г) Фишинг
14. Какой механизм НЕ используется для защиты ОС?
а) Шифрование
б) Аутентификация
в) Фрагментация памяти
г) Аудит
15. Какая ОС использует микроядро?
а) Windows 10
б) Linux
в) macOS
г) QNX

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»

ПК 1.1.: Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

Недостаточный уровень:
Знает отдельные названия компонентов автоматизированной системы (процессор, память, диск, программа), названия операционных систем (Windows, Linux), элементарные понятия алгоритма (последовательность действий), названия моделей баз данных (реляционная), а также названия периферийных устройств (принтер, сканер, клавиатура).

Умеет под руководством преподавателя подбирать компоненты АС по списку, выполнять базовую настройку BIOS (загрузка с диска), устанавливать антивирус по инструкции, а также создавать простую учётную запись пользователя с паролем.

Имеет практический опыт запуска установки антивируса по инструкции, следования указаниям установщика (нажатие «Далее») под контролем, ввода лицензионного ключа по образцу, а также включения базовой защиты (брандмауэр) по инструкции.

Пороговый уровень:
Знает состав автоматизированных систем (аппаратное и программное обеспечение, пользователи, информационные и организационные подсистемы) и принципы их работы (взаимодействие компонентов, обработка данных, управление); принципы работы операционных систем (управление процессами, памятью, файловой системой, вводом-выводом) и сред (среды разработки, виртуализации); принципы разработки алгоритмов программ (последовательность, ветвление, цикл, подпрограммы, рекурсия) и основные приёмы программирования (структурное, модульное, объектно-ориентированное); модели баз данных (иерархическая, сетевая, реляционная, NoSQL); принципы построения и физические основы работы периферийных устройств (принтеры: матричные, струйные, лазерные; сканеры: планшетные, протяжные; клавиатура, мышь, монитор, дисководы) – преобразование сигналов, интерфейсы подключения, драйверы.

Умеет самостоятельно комплектовать автоматизированную систему в защищённом исполнении (выбор оборудования, проверка совместимости), выполнять конфигурирование и настройку (BIOS/UEFI, установка ОС, настройка сетевых параметров, политик безопасности), устанавливать и настраивать компоненты систем защиты информации (антивирус, межсетевой экран, контроль доступа, резервное копирование), а также

Умеет самостоятельно комплектовать автоматизированную систему в защищённом исполнении (выбор оборудования, проверка совместимости), выполнять конфигурирование и настройку (BIOS/UEFI, установка ОС, настройка сетевых параметров, политик безопасности), устанавливать и настраивать компоненты систем защиты информации (антивирус, межсетевой экран, контроль доступа, резервное копирование), а также обеспечивать базовые требования защищённого исполнения (изоляция, минимальные привилегии, аудит).

Имеет практический опыт установки и настройки компонентов СЗИ (антивирус, межсетевой экран, контроль доступа, резервное копирование), выполнения базовой настройки (политики, правила, права, расписания), проверки совместимости, обновления баз и лицензий, а также тестирования работоспособности установленных компонентов.

Продвинутый уровень:
Знает архитектуру автоматизированных систем (распределённые, клиент-серверные, встроенные), внутреннее устройство ОС (ядро, драйверы, системные вызовы), методы оценки сложности алгоритмов (О-нотация), особенности различных моделей БД (нормализация, транзакции, индексы), а также физические принципы работы устройств на уровне электроники и механики (формирование изображения, считывание, преобразование сигналов).

Умеет самостоятельно комплектовать и настраивать защищённые АС для различных классов защищённости (по требованиям ФСТЭК), конфигурировать СЗИ (политики доступа, правила фильтрации, настройки аудита, VPN), интегрировать компоненты СЗИ в единую систему, а также проводить проверку работоспособности средств защиты и тестирование на соответствие требованиям.

Имеет практический опыт установки и настройки сертифицированных СЗИ (СКЗИ, DLP, IDS/IPS) под различные ОС (Windows, Linux, Astra Linux), настройки компонентов для требуемого класса защищённости, оптимизации производительности СЗИ, проверки корректности установки и настройки, а также интеграции компонентов СЗИ в единую систему (централизованное управление, сбор событий).

Высокий уровень:
Знает современные архитектуры АС (микросервисные, событийно-ориентированные, edge computing), основы построения операционных систем реального времени и распределённых ОС, методологию разработки сложных алгоритмов и программных систем (ООП, паттерны), модели БД нового поколения (NewSQL, графовые, временные ряды, векторные), а также физические основы работы новейших периферийных устройств (3D-принтеры, сенсорные экраны, биометрические сканеры, VR-устройства).

Умеет самостоятельно проектировать и настраивать защищённые АС для объектов критической информационной инфраструктуры, внедрять современные СЗИ (EDR, NGFW, SIEM, DLP), проводить оценку эффективности защиты, выполнять настройку в соответствии с нормативными требованиями (ГОСТ, приказы ФСТЭК), а также обучать других комплектованию, конфигурированию и настройке защищённых АС.

Имеет практический опыт внедрения комплексных СЗИ в корпоративной инфраструктуре (SIEM, EDR, DLP), настройки централизованного управления СЗИ (агентские/безагентные решения), автоматизации развёртывания и настройки СЗИ (скрипты, групповые политики), интерпретации требований нормативных документов (ФСТЭК) при установке и настройке, а также обучения других установке и настройке компонентов СЗИ.

Перечень практических навыков, приобретаемых при изучении дисциплины:

ПК 1.1: Иметь навыки установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2: Иметь навыки администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3: Иметь навыки обеспечения бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4: Иметь навыки и опыт деятельности по проверке технического состояния, техническому обслуживанию, текущему ремонту, устранению отказов и восстановлению работоспособности автоматизированных (информационных) систем в защищенном исполнении.

Методы оценки	Критерии оценки
Экспертное наблюдение за решением обучающимися проблемно-ситуационных задач в рамках практической подготовки	Оценка «отлично» – задание выполнено полностью, в рамках регламента, установленного на публичную презентацию, студент(ы) приводит (подготовили) полную четкую аргументацию выбранного решения на основе качественно сделанного анализа задания. Демонстрируются хорошие теоретические знания, имеется собственная обоснованная точка зрения на проблему(ы) и причины ее (их) возникновения. В случае ряда выявленных проблем четко определяет их иерархию. При устной презентации уверенно и быстро отвечает на заданные вопросы, выступление сопровождается приемами визуализации. В случае письменного отчета-презентации по выполнению кейс-задания сделан структурированный и детализированный анализ, представлены возможные варианты решения (3-5), четко и аргументировано обоснован окончательный выбор одного из альтернативных решений. Оценка «хорошо» – задание выполнено полностью, но в рамках установленного на выступление регламента, студент(ы) не приводит (не подготовили) полную четкую аргументацию выбранного решения. Имеет место излишнее теоретизирование, или наоборот, теоретическое обоснование ограничено, имеется собственная точка зрения на проблемы, но не все причины ее возникновения установлены.

	При устной презентации на дополнительные вопросы выступающий отвечает с некоторым затруднением, подготовленная устная презентации выполненного задания не очень структурирована. При письменном отчете-презентации по выполнению задания сделан неполный анализ, без учета ряда фактов, выявлены не все возможные проблемы, для решения могла быть выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 2-3, затруднена четкая аргументация окончательного выбора одного из альтернативных решений. Оценка «удовлетворительно» – задание выполнено более чем на 2/3, но в рамках установленного на выступление регламента, студент(ы) расплывчато раскрывает решение, не может четко аргументировать сделанный выбор, показывает явный недостаток теоретических знаний. Выводы слабые, свидетельствуют о недостаточном анализе фактов, в основе решения может иметь место интерпретация фактов или предположения, собственная точка зрения на причины возникновения проблемы не обоснована или отсутствует. При устной презентации на вопросы отвечает с трудом или не отвечает совсем. Подготовленная презентация выполненного задания не структурирована. В случае письменной презентации по выполнению кейсзадания не сделан детальный анализ, далеко не все факты учтены, для решения выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 1-2, отсутствует четкая аргументация окончательного выбора решения. Оценка «неудовлетворительно» – задание не выполнено, или выполнено менее чем на треть. Отсутствует детализация при анализе задания, изложение устное или письменное не структурировано. Если решение и обозначено в выступлении или отчете-презентации, то оно не является решением проблемы, которая заложена в задании.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

5.1.1. Основная литература

Л.1.1	Иванько А. Ф., Иванько М. А., Курносова А. В. Операционные системы. Практикум [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2022. - 132 с. – Режим доступа: https://e.lanbook.com/book/266765
Л.1.2	Староверова Н. А. Операционные системы [Электронный ресурс]:учебник. - Санкт-Петербург: Лань, 2022. - 308 с. – Режим доступа: https://e.lanbook.com/book/207089
Л.1.3	Староверова Н. А. Операционные системы [Электронный ресурс]:. - Санкт-Петербург: Лань, 2022. - 412 с. – Режим доступа: https://e.lanbook.com/book/186048
Л.1.4	Исаева Г. Н., Сидорова Н. П. Операционные системы, среды и оболочки: практикум [Электронный ресурс]:учебное пособие. - Москва: Директ-Медиа, 2022. - 51 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=693549
Л.1.5	Исаева Г. Н. Операционные системы, среды и оболочки: методические указания по выполнению курсовой работы [Электронный ресурс]:методическое пособие. - Москва: Директ-Медиа, 2022. - 25 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=693539
Л.1.6	Тенгайкин Е. А. Организация сетевого администрирования. Сетевые операционные системы, серверы, службы и протоколы. Практические работы [Электронный ресурс]:Учебное пособие для СПО. - Санкт-Петербург: Лань, 2022. - 100 с. – Режим доступа: https://e.lanbook.com/book/198497
Л.1.7	Малахов С. В. Операционные системы и оболочки [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2023. - 120 с. – Режим доступа: https://e.lanbook.com/book/302681
Л.1.8	Куль Т. П. Операционные системы. Программное обеспечение [Электронный ресурс]:учебник для спо. - Санкт-Петербург: Лань, 2023. - 248 с. – Режим доступа: https://e.lanbook.com/book/292994
Л.1.9	Малахов С. В. Операционные системы и оболочки [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2023. - 120 с. – Режим доступа: https://e.lanbook.com/book/302690
Л.1.10	А.В. Батаев и др. Операционные системы и среды:учебник. - Москва: Издательский центр "Академия", 2023. - 288 с.
Л.1.11	Иванько А. Ф., Иванько М. А., Курносова А. В. Операционные системы. Практикум [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2023. - 132 с. – Режим доступа: https://e.lanbook.com/book/354521

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 18-1302 - 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;

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

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.

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.

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 _____

==========