Министерство образования и науки Республики Татарстан
Государственное автономное профессиональное образовательное учреждение
«Сабинский аграрный колледж»

РАССМОТРЕНО на заседании
предметной (цикловой) комиссии
Протокол № 4 от 15 апреля 2026 года

ОДОБРЕНО
на заседании Педагогического совета
ГАПОУ «САК»
протоколом №29 от «16» апреля 2026 года

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ОП.02 Операционные системы и среды

по специальности

09.02.11 «Разработка и управление программным обеспечением»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 1E093667AA5CBF33044A6008CC579BE5
Владелец: Бикмухаметов Закиржан Миннемуллович
Действителен с 02.09.2025 до 26.11.2026

2026

Структура контрольных заданий

1. Задания текущего контроля

Текущий контроль качества обученности студентов осуществляется в форме выполнения тестов по теории и практических заданий.

Практическая работа №1 «Журнал аудита»

Задание 1. Настройка политики аудита.

Цель задания: Научиться настраивать политики аудита для отслеживания конкретных событий в Windows. Таких как вход в систему, доступ к файлам и изменения в политиках безопасности.

Шаг 1. Открыть оснастку «Локальная политика безопасности». Для того, чтобы ее открыть:

1. Нажмите комбинацию клавиш Win+R, откроется окно «Выполнить».
2. Введите команду secpol.msc и нажмите ОК.

Шаг 2. Перейти к разделу «Политика аудита». Для того, чтобы перейти к ней:

1. В левой панели оснастки «Локальная политика безопасности» разверните раздел «Локальные политики».
2. Выберите подраздел «Политика аудита». На правой панели отобразятся все доступные категории событий, которые можно аудировать в системе.

Шаг 3. Настройка аудита для событий входа в систему. Для того, чтобы провести настройку, необходимо:

1. Найдите в списке политику «Аудит входа в систему».
2. Дважды щелкните по ней – откроются свойства.
3. В открывшемся окне необходимо установить флажки «Успех» и «Отказ» для того, чтобы отслеживать все успешные и неудачные попытки входа в систему.
4. Нажмите «Применить», а затем «ОК».

Итог настройки: Система будет отслеживать, кто и когда успешно/неуспешно пытался войти в систему, а также фиксировать попытки несанкционированного доступа»

Шаг 4. Настройка аудита доступа к объектам (файлам и папкам). Для того, чтобы настроить данный аудит, необходимо:

1. Найдите в списке политику «Аудит доступа к объектам».
2. Дважды щелкните по ней – откроются свойства.
3. В открывшемся окне необходимо установить флажки «Успех» и «Отказ» для того, чтобы отслеживать все успешные и неуспешные попытки доступа к файлам и папкам.
4. Нажмите «Применить», а затем «ОК».

Итог настройки: Система будет отслеживать, кто и какие файлы или папки открывал, изменял или пытался получить к ним доступ.

Шаг 5. Настройка аудита изменений в политиках безопасности. Для того, чтобы провести данную настройку, необходимо:

1. Найдите в списке политику «Аудит изменения политики».
2. Дважды щелкните по ней – откроются свойства.
3. В открывшемся окне необходимо установить флажки «Успех» и «Отказ» для того, чтобы отслеживать все успешные и неуспешные попытки изменения в политиках безопасности.
4. Нажмите «Применить», а затем «ОК».

Итог настройки: Система будет отслеживать, кто и когда вносил изменения в политики безопасности, что важно для контроля целостности системы.

Шаг 6. Закройте оснастку «Локальная политика безопасности».

Шаг 7. Проверка настроек. Для того, чтобы проверить все выполненные настройки, необходимо:

1. Попробуйте выполнить действия, которые вы настроили для аудита (например, войдите в систему или откройте какой-нибудь файл).

2. Откройте «Просмотр событий» (найти через поисковик или Win + R и выполнить eventvwr.msc).
3. На левой панели необходимо выбрать раздел «Журналы Windows».
4. В данном разделе необходимо перейти к подразделу «Безопасность».
5. В данном подразделе будут отображаться все соответствующие события.

Вопросы:

1. Какие еще категории событий можно аудировать? Приведите примеры.
2. Почему важно отслеживать как успешные, так и неудачные попытки доступа?
3. Как можно использовать журнал аудита для расследования инцидентов безопасности?

Задание 2. Аудит доступа к конкретному файлу или папке.

Цель задания: Научиться настраивать аудит для конкретных файлов или папок.

Шаг 1. Создайте папку на рабочем столе с названием «TestAudit».

Шаг 2. Щелкните правой кнопкой мыши на папке и выберите «Свойства».

Шаг 3. Перейдите на вкладку «Безопасность» и нажмите кнопку «Дополнительно».

Шаг 4. В открывшемся окне перейдите на вкладку «Аудит».

Шаг 5. Нажмите кнопку «Добавить».

Шаг 6. В поле «Субъект» введите «Все» и нажмите «ОК».

Шаг 7. В следующем окне выберите:

— Тип: «Все».

— Применяется к: «Для этой папки, ее подпапок и файлов».

— В разделе «Общие разрешения» выберите действия «Чтение», «Запись» и «Изменение».

Шаг 8. Сохраните изменения.

Шаг 9. Попробуйте выполнить действия с папкой (например, создайте файл, переименуйте его, откройте файл).

Шаг 10. Проверьте журнал безопасности в «Просмотре событий» на наличие событий с Кодом события 4663 (доступ к объекту).

Вопрос: Какие действия были зафиксированы в журнале? Как можно использовать эту информацию для мониторинга доступа к конфиденциальным данным?

Задание 3. Фильтрация событий в журнале безопасности.

Цель задания: Научиться фильтровать события в журнале безопасности для быстрого поиска нужной информации.

Шаг 1. Откройте «Просмотр событий» (Win + R -> eventvwr.msc).

Шаг 2. Перейдите в раздел «Журналы Windows» -> «Безопасность».

Шаг 3. В правой панели нажмите «Фильтр текущего журнала».

Шаг 4. В открывшемся окне укажите **Код события**, например, 4624 (успешный вход в систему). Выберите временной диапазон (например, последние 30 дней).

Шаг 5. Нажмите «ОК».

Шаг 6. Изучите отфильтрованные события.

Шаг 7. Повторите фильтрацию для других событий, например:

— **4625** (неудачный вход в систему).

— **4663** (доступ к объекту).

— **4672** (использование привилегий).

Вопрос: Как фильтрация событий помогает в анализе журналов? Какие еще параметры можно использовать для фильтрации?

Задание 4. Экспорт и анализ журнала безопасности.

Цель задания: Научиться экспортировать журнал безопасности для дальнейшего анализа.

Шаг 1. Откройте «Просмотр событий» (Win + R -> eventvwr.msc).

Шаг 2. Перейдите в раздел «Журналы Windows» -> «Безопасность».

Шаг 3. В правой панели нажмите «Сохранить все события как…».

Шаг 4. Выберите место для сохранения и укажите имя файла (например, SecurityLog.evtx).

Шаг 5. Экспортируйте журнал в формате .evtx.

Шаг 6. Откройте экспортированный файл в «Просмотре событий» (через меню «Действие» -> «Открыть сохраненный журнал»).

Шаг 7. Проведите анализ событий, используя фильтры (как в Задании 3).

Шаг 8. Удалите загруженный журнал с помощью меню «Действие» -> «Удалить».

Задание 5. Настройка размера журнала безопасности.

Цель задания: Научиться управлять размером журнала безопасности и его поведением при переполнении.

Шаг 1. Откройте «Просмотр событий» (Win + R -> eventvwr.msc).

Шаг 2. Перейдите в раздел «Журналы Windows» -> «Безопасность».

Шаг 3. Щелкните правой кнопкой мыши на журнале «Безопасность» и выберите «Свойства».

Шаг 4. В открывшемся окне:

— Установите максимальный размер журнала (например, 100 МБ).

— Выберите действие при достижении максимального размера: Архивировать журнал при заполнении; не перезаписывать события.

Шаг 5. Сохраните изменения.

Вопрос: Какие параметры настройки журнала безопасности наиболее важны для обеспечения непрерывного аудита? Почему?

Практическая работа №2. Политика безопасности.

Цель работы: Изучить основные механизмы настройки и управления политиками безопасности в Windows 10, а также понять их роль в обеспечении защиты системы и данных.

Теория: Политика безопасности — это набор правил и настроек, которые определяют, как система управляет доступом к ресурсам, защищает данные и контролирует действия пользователей.

Основные компоненты политики безопасности в Windows 10:

— Управление учетными записями пользователей (UAC).

— Настройка прав доступа к файлам и папкам.

— Использование групповых политик (GPO).

— Настройка брандмауэра Windows.

— Шифрование данных (BitLocker).

— Аудит событий безопасности.

— Защита от вредоносных программ (Windows Defender).

Задание 1. Настройка контроля учетных записей (UAC)

Шаг 1. Откройте «Панель управления» → «Учетные записи пользователей» → «Изменить параметры контроля учетных записей».

Шаг 2. Изучите текущие настройки UAC. Измените уровень уведомлений на «Всегда уведомлять» и сохраните изменения.

Шаг 3. Запустите программу, требующую прав администратора. Обратите внимание на поведение системы. (Например, зайдите обратно в настройки UAC, поскольку теперь система уведомляет на любое изменение параметров, то выведется соответствующее сообщение).

Шаг 4. Верните настройки UAC в исходное состояние.

Вопрос: Как уровень UAC влияет на безопасность системы и удобство работы пользователя?

Задание 2. Настройка прав доступа к файлам и папкам

Шаг 1. Создайте папку на рабочем столе с именем «TestFolder».

Шаг 2. Щелкните правой кнопкой мыши на папке → «Свойства» → вкладка «Безопасность».

Шаг 3. Изучите список пользователей и групп, имеющих доступ к папке. Добавьте нового пользователя (или группу) и настройте для него права доступа (например, «Чтение и выполнение»).

Шаг 4. Попробуйте открыть папку с учетной записи, для которой вы ограничили права. Что происходит?

Вопрос: Какие риски возникают при неправильной настройке прав доступа к файлам и папкам?

Задание 3. Работа с локальной групповой политикой

Шаг 1. Откройте редактор локальной групповой политики:

Шаг 2. Нажмите Win + R, введите gpedit.msc и нажмите Enter.

Шаг 3. Перейдите в раздел: «Конфигурация компьютера» → «Конфигурация Windows» → «Параметры безопасности» → «Локальные политики» → «Политика аудита».

Шаг 4. Включите аудит успешных и неудачных попыток входа в систему.

Шаг 5. Попробуйте войти в систему с неверным паролем, а затем с правильным.

Шаг 6. Проверьте журнал событий (Win + R → eventvwr.msc → «Журналы Windows» → «Безопасность») и найдите записи о попытках входа.

Вопрос: Как аудит событий помогает администратору в обеспечении безопасности системы?

Задание 4. Настройка брандмауэра Windows

Шаг 1. Откройте «Панель управления» → «Система и безопасность» «Брандмауэр Защитника Windows».

Шаг 2. Изучите текущие настройки брандмауэра. Создайте новое правило для входящих подключений, разрешающее доступ к определенному порту (например, порт 8080).

1. В левой панели выберите «Дополнительные параметры»
2. Откроется «Монитор брандмауэра Защитника Windows в режиме повышенной безопасности».
3. В левой панели выберите «Правила для входящих подключений».
4. В меню «Действия» выберите «Создать правило…».
5. Откроется «Мастер создания правила для нового входящего подключения».
6. В открывшемся окне выберите «Тип правила» → «Для порта». Нажмите «Далее».
7. Выберите тип протокола:
   — TCP (если ваш сервис использует TCP, например, веб-сервер).
   — UDP (если ваш сервис использует UDP, например, потоковое видео).
8. Выберите Определенные локальные порты и введите номер порта. Нажмите «Далее».
9. Выберите «Разрешить подключение». Нажмите «Далее».
10. Укажите, когда применяется это правило:
    — Домен (если компьютер подключен к домену).
    — Частная (если компьютер в частной сети, например, дома).
    — Публичная (если компьютер в публичной сети, например, в кафе).
11. Выберите нужные профили (обычно можно оставить все три) и нажмите «Далее».
12. Введите имя правила. При необходимости добавьте описание.

13. Нажмите Готово.

Вопрос: Какие угрозы могут возникнуть при неправильной настройке брандмауэра?

Задание 5. Настройка Windows Defender

Шаг 1. Откройте «Безопасность Windows».

Шаг 2. Проверьте статус защиты от вирусов и угроз. Запустите полное сканирование системы.

Шаг 3. Изучите настройки защиты от программ-шантажистов и настройте ее.

Шаг 4. Проверьте «Журнал защиты» и изучите обнаруженные объекты.

Вопрос: Как Windows Defender помогает защитить систему от современных угроз?

Задание 6. Создание и настройка учетных записей пользователей

Шаг 1. Откройте «Панель управления» → «Учетные записи пользователей» → «Управление другой учетной записью».

Шаг 2. Создайте новую учетную запись с ограниченными правами.

Шаг 3. Настройте пароль для новой учетной записи и ограничьте доступ к определенным папкам.

Шаг 4. Проверьте работу учетной записи, войдя в систему под новым пользователем.

Вопрос: Какие меры безопасности следует учитывать при создании и настройке учетных записей пользователей?

Задание 7: Настройка политик паролей

Шаг 1. Откройте «Редактор локальной групповой политики» (gpedit.msc).

Шаг 2. Перейдите в раздел: «Конфигурация компьютера» → «Конфигурация Windows» → «Параметры безопасности» → «Политики учетных записей» → «Политика паролей».

Шаг 3. Настройте требования к паролям: минимальная длина, сложность, срок действия.

Шаг 4. Проверьте, как новые настройки влияют на создание паролей.

Вопрос: Какие рекомендации можно дать пользователям по созданию надежных паролей?

Практическая работа №3. Файл подкачки

Цель: Изучить принципы работы файла подкачки в Windows, научиться настраивать его параметры и анализировать влияние на производительность системы.

Теоретическая часть: **Файл подкачки (pagefile.sys)** — это специальный файл на жестком диске, который используется операционной системой Windows для расширения оперативной памяти (ОЗУ). Когда физической памяти не хватает, система перемещает неиспользуемые данные из ОЗУ в файл подкачки, освобождая место для активных процессов.

Основные понятия:

Виртуальная память — совокупность оперативной памяти и файла подкачки.

Свопинг — процесс перемещения данных между ОЗУ и файлом подкачки.

Рекомендуемый размер файла подкачки — обычно 1,5–2 раза больше объема ОЗУ.

Задание 1. Проверка текущих настроек файла подкачки.

Шаг 1. Откройте «Панель управления» → «Система и безопасность» → «Система».

Шаг 2. Откроются «Параметры». В левом меню выберите «О программе» → «Дополнительные параметры системы».

Шаг 3. В открывшемся окне перейдите на вкладку «Дополнительно» и в разделе «Быстродействие» нажмите «Параметры…».

Шаг 4. В новом окне выберите вкладку «Дополнительно» и в разделе «Виртуальная память» нажмите «Изменить».

Шаг 5. Отобразите на скриншоте текущие настройки:

— Размер файла подкачки (например, «По выбору системы» или указан вручную).

— Расположение файла подкачки (на каком диске).

Задание 2. Изменение файла подкачки.

В том же окне Виртуальная память:

Шаг 1. Снимите галочку «Автоматически выбирать объем файла подкачки».

Шаг 2. Выберите «Указать размер» и задайте:

— Исходный размер: 2048 МБ.

— Максимальный размер: 4096 МБ.

Шаг 3. Нажмите «Задать», затем «ОК».

Шаг 4. Перезагрузите компьютер.

Задание 3. Анализ использования файла подкачки.

Шаг 1. После перезагрузки откройте «Диспетчер задач» (Ctrl + Shift + Esc).

Шаг 2. Перейдите на вкладку «Производительность» и выберите «Память».

Шаг 3. Обратите внимание на параметры:

— Используемая память.

— Доступная память.

— Размер файла подкачки.

Шаг 4. Запустите несколько ресурсоемких приложений (например, браузер с множеством вкладок).

Шаг 5. Наблюдайте за изменением использования памяти и файла подкачки.

Задание 4. Отключение файла подкачки

Шаг 1. Вернитесь в окно Виртуальная память.

Шаг 2. Выберите «Без файла подкачки» и нажмите «Задать».

Шаг 3. Перезагрузите компьютер.

Шаг 4. Повторите шаги из **задания 3**. Сравните производительность системы с включенным и отключенным файлом подкачки.

Вопросы:

Как изменилась производительность системы при уменьшении размера файла подкачки?

Что произошло при отключении файла подкачки?

В каких случаях рекомендуется увеличивать размер файла подкачки?

Сделайте выводы о роли файла подкачки в работе операционной системы.

Вывод:

Практическая работа №4. Монитор стабильности Windows

Цель: Ознакомиться с инструментом «Монитор стабильности системы» в Windows 10, научиться анализировать стабильность работы системы, выявлять причины сбоев и устранять их. Развить навыки диагностики и оптимизации работы операционной системы.

Необходимая теория:

Монитор стабильности — это встроенный инструмент Windows 10, который позволяет отслеживать события, влияющие на стабильность системы (сбои приложений, ошибки оборудования, обновления и т.д.).

Он предоставляет визуальный график стабильности системы и детализированные отчеты о событиях.

Задание 1. Запустите монитор стабильности.

Шаг 1. Нажмите Win + R, введите команду perfmon /rel и нажмите Enter.

Шаг 2. Откроется окно «Монитор стабильности системы». Обратите внимание на график. Он показывает стабильность системы за последние несколько дней.

Шаг 3. Изучите график: красные точки обозначают критические события (сбои, ошибки), желтые треугольники обозначают предупреждения (незначительные ошибки) и синие отображают сведения в системе.

Задание 2. Анализ события. Часть 1.

Шаг 1. Выберите день на графике с красной точкой.

Шаг 2. В нижней части окна появится события, которые произошли в этот день.

Шаг 3. Изучите типы событий:

— Ошибки приложений – сбои в работе программ.

— Ошибки Windows – сбои в работе операционной системы.

— Другие сбои – например, неправильное завершение работы ПК.

Шаг 4. Нажмите на одна из событий, чтобы увидеть подробную информацию.

Шаг 5. Заполните таблицу

Тип события	Описание ошибки	Возможные причины (если указаны)

Задание 3. Анализ события. Часть 2.

Шаг 1. Создайте искусственную ошибку:

— Запустите программу, которая может вызвать сбой (например, текстовый редактор или браузер).

— Закройте программу через диспетчер задач.

Шаг 2. Откройте монитор стабильности снова.

Шаг 3. Найдите событие, связанное с вашим действием.

Шаг 4. Проанализируйте событие:

— Как оно отображается на графике?

— Какое описание ошибки указано?

Шаг 5. Попробуйте устранить проблему: Переустановите программу, которая вызвала сбой. Проверьте исчезла ли ошибка в мониторе стабильности.

Задание 4. Раздел действия в «Мониторе стабильности системы».

Шаг 1. Изучите раздел «Действия» в мониторе стабильности.

Шаг 2. Найдите информацию о последних обновлениях системы и их влиянии на стабильность.

Шаг 3. Запишите какие обновления были установлены и как они повлияли на систему.

Вопросы:

1. Какие типы событий отслеживает монитор стабильности?
2. Как можно использовать этот инструмент для диагностики проблем?
3. Какие действия можно предпринять для повышения стабильности системы?

Тест по введению в операционные системы:

Время на выполнение: _30_ мин.

1. Что такое операционная система (ОС)?

a) Программа для создания текстовых документов

b) Комплекс программного обеспечения, который управляет аппаратными ресурсами компьютера

c) Программа для редактирования фотографий

d) Система для управления базами данных

2. Какова основная цель операционной системы?

a) Управлять подключением к интернету

b) Обеспечить эффективную и безопасную работу программ и приложений

c) Редактировать текстовые документы

d) Управлять доступом к базам данных

3. Какое требование НЕ относится к современным операционным системам?

a) Высокая производительность

b) Поддержка вывода изображения в формате 3D

c) Масштабируемость

d) Безопасность

4. Какая из следующих классификаций операционных систем является верной?

a) По цвету интерфейса

b) По количеству одновременных пользователей

c) По количеству окон на экране

d) По размеру файла установки

5. Что относится к системному программному обеспечению, помимо операционных систем?

a) Программы для создания графики

b) Системные утилиты

c) Игры

d) Браузеры

6. Какие операционные системы предназначены для мобильных устройств? (Выберите все подходящие ответы)

a) Windows

b) iOS

c) Android

d) Mac OS

7. Как называются модули операционной системы, которые выполняют основные функции ОС?

a) Вспомогательные модули

b) Утилиты

c) Ядро

d) Драйверы

8. Что включает в себя ядро операционной системы?

a) Только управление вводом-выводом

b) Управление процессами, памятью и вводом-выводом

c) Только управление памятью

d) Обработку системных вызовов

9. Какую задачу выполняет ядро ОС при управлении процессами?

a) Управление виртуальной памятью

b) Архивирование файлов

c) Создание, переключение и завершение процессов

d) Подключение периферийных устройств

10. Как называется механизм, с помощью которого приложения обращаются к ядру для выполнения действий, таких как открытие файла или вывод данных?

a) Драйвер

b) Виртуальная машина

c) Системный вызов

d) Компилятор

11. Какие задачи решают вспомогательные модули операционной системы?

a) Управление процессами и памятью

b) Сопровождение программ и взаимодействие пользователя с системой (правильный ответ)

c) Только обработка графической информации

d) Управление сетевыми интерфейсами

12. Назовите компонент операционной системы, который управляет выделением и освобождением памяти для программ.

a) Сетевой интерфейс

b) Вспомогательные модули

c) Ядро

d) Утилиты

13. Какие задачи выполняют утилиты в операционной системе?

a) Управление процессами и потоками

b) Решают задачи управления и сопровождения компьютерной системы, такие как архивирование и сжатие данных

c) Управление сетевыми интерфейсами

d) Запуск приложений на виртуальной машине

14. Что предоставляют программы дополнительных услуг в операционной системе?

a) Управление вводом-выводом

b) Дополнительные функции для пользователя, такие как калькулятор или игры

c) Создание и завершение процессов

d) Управление доступом к файлам

15. Какое свойство операционной системы обеспечивает защиту кода и данных?

a) Пользовательский режим

b) Прерывания

c) Привилегированный режим

d) Системный таймер

16. Какое из перечисленных средств аппаратной поддержки ОС отвечает за управление контекстом процессов?

a) Виртуальная память

b) Системный таймер

c) Привилегированный режим

d) Переключение контекста

17. Какая структура ОС обеспечивает доступ только к нижележащему уровню через его интерфейс?

a) Многозадачная структура

b) Многослойная структура

c) Монолитная структура

d) Клиент-серверная структура

18. Что позволяет ОС управлять временем выполнения задач?

a) Виртуальная память

b) Прерывания

c) Системный таймер

d) Менеджер ресурсов

19. Какую роль выполняет базовый слой ядра в многослойной структуре ОС?

a) Решает стратегические задачи

b) Выполняет системные вызовы

c) Исполняет принятые решения верхних слоев

d) Обрабатывает прерывания

20. Что делает менеджер ресурсов в операционной системе?

a) Управляет процессами на уровне приложений

b) Реализует стратегию распределения ресурсов

c) Синхронизирует работу устройств

d) Управляет прерываниями

21. Какой уровень в многослойной архитектуре ядра ОС взаимодействует с приложениями?

a) Интерфейс системных вызовов

b) Менеджер ресурсов

c) Базовые механизмы

d) Машинно-зависимые модули

22. Какая функция ОС инициирует переключение процессора из

пользовательского режима в привилегированный?

a) Прерывание

b) Системный вызов

c) Менеджер памяти

d) Переключение контекста

23. Как называется регистр, содержащий признаки режимов работы CPU?

a) Таймер процесса

b) Регистр состояний

c) Слово состояния машины

d) Адресный регистр

24. Какая функция ОС преобразует виртуальные адреса в физические?

a) Привилегированный режим

b) Виртуальная память

c) Переключение контекста

d) Прерывания

Ключи к тестам

1) b

2) b

3) b

4) b

5) b

6) b, c

7) c

8) b

9) c

10) c

11) b

12) c

13) b

14) b

15) c

16) d

17) b

18) c

19) c

20) b

21) a

22) b

23) c

24) b

Критерии оценки

Процент результативности (правильных ответов)	**Оценка уровня подготовки**	
	балл (отметка)	**вербальный аналог**
21 - 24	5	отлично
17 - 20	4	хорошо
12 - 16	3	удовлетворительно
менее 12	2	неудовлетворительно

Тест по процессам и потокам в операционных системах:

Время на выполнение: _45_ мин.

1. Что такое процесс?

a) Набор функций, выполняемых параллельно

b) Исполняемая программа в операционной системе

c) Операция ввода-вывода

d) Поток данных между двумя процессами

2. Какое свойство не вытесняющего алгоритма планирования?

a) Задача выполняется до тех пор, пока сама не освободит процессор

b) Задача может быть прервана для выполнения другой задачи

c) Задача получает фиксированный квант времени

d) Задачи распределяются по приоритетам

3. Какое из перечисленных действий выполняется ОС при переключении задач?

a) Запись содержимого файлов

b) Сохранение контекста текущего процесса

c) Завершение активных потоков

d) Освобождение системной памяти

4. Что означает "дисциплина диспетчеризации"?

a) Правила выделения памяти процессам

b) Правила формирования очереди готовых к выполнению задач

c) Правила обработки прерываний

d) Метод работы устройств ввода-вывода

5. Что характеризует статическое планирование?

a) Принимает решения в процессе работы системы

b) Принимает решения заранее на основе известных задач

c) Использует динамические приоритеты

d) Изменяет приоритеты задач во время выполнения

6. Что характеризует динамическое планирование?

a) Используется в системах реального времени

b) Применяется только к простым задачам

c) Принимает решения на основе текущей ситуации во время

работы системы

d) Формирует расписание задач перед запуском системы

7. Какое из следующих утверждений относится к диспетчеризации с динамическими приоритетами?

a) Приоритет задачи фиксирован на протяжении всего выполнения

b) Приоритет задачи изменяется во время выполнения

c) Задачи выполняются по кругу, сменяя друг друга

d) Каждая задача получает равные кванты времени

8. Что такое контекст процесса?

a) Набор инструкций для выполнения задачи

b) Состояние аппаратуры и операционной среды процесса

c) Механизм управления памятью

d) Место в очереди на выполнение

9. Какой из нижеперечисленных методов является вытесняющим алгоритмом планирования?

a) SJN

b) RR

c) FCFS

d) SRT

10. Какое преимущество дисциплины FCFS?

a) Задачи с малым временем выполнения выполняются первыми

b) Низкие накладные расходы на обработку очереди

c) Задачи вытесняются при необходимости

d) Гарантированное завершение коротких задач быстрее

11. В чем основное отличие между вытесняющими и не

вытесняющими алгоритмами?

a) Время выполнения задачи

b) Распределение процессорного времени

c) Взаимодействие задач с памятью

d) Степень централизации планирования

12. Что такое поток?

a) Независимый процесс, выполняющий задачу

b) Логическая часть процесса, выполняющаяся параллельно

c) Задача диспетчера процессов

d) Механизм обработки сигналов в ОС

13. Что происходит при динамическом планировании?

a) Решения принимаются до начала работы системы

b) Решения принимаются во время работы системы на основе текущих условий

c) Все задачи имеют фиксированный приоритет

d) Задачи распределяются на основе заранее составленного расписания

14. Какой из следующих элементов сохраняется при переключении контекста?

a) Код программы

b) Значение счетчика команд

c) Таблица файлов

d) Оперативная память

15. В каком состоянии может находиться поток, если ему нужно дождаться завершения операции ввода-вывода?

a) Выполнение

b) Ожидание

c) Готовность

d) Прерывание

16. Какой основной недостаток дисциплины SJN?

a) Сложность реализации

b) Короткие задачи могут вытеснять длинные

c) Длительные задачи могут ждать долгое время

d) Задачи с высоким приоритетом выполняются медленнее

17. Что определяет момент снятия текущей задачи с процессора в вытесняющих алгоритмах?

a) Время выполнения задачи

b) Решение операционной системы

c) Само завершение задачи

d) Время ожидания в очереди

18. Как операционная система выбирает задачу для выполнения в не вытесняющих алгоритмах?

a) Задачи вытесняются по времени выполнения

b) Операционная система сама выбирает задачи на основе приоритетов

c) Активная задача самостоятельно отдает управление системе

Используется статическое планирование

19. В чем заключается основное назначение статического планирования?

a) Ускорение выполнения задач

b) Снижение времени переключения контекстов

c) Создание расписания выполнения задач заранее

d) Автоматическая настройка приоритетов задач

20. Какой тип планирования обычно используется в системах реального времени?

a) Статическое планирование

b) Динамическое планирование

c) FCFS

d) SRT

21. Что из перечисленного является примером функции ОС при вытесняющем планировании?

a) Освобождение процессорного времени задачей по её инициативе

b) Сохранение и загрузка контекста задач

c) Построение расписания задач перед запуском системы

d) Предоставление процессорного времени только одной задаче

22. Какое из состояний относится к процессу?

a) Готовность

b) Подготовка

c) Передача

d) Обработка

23. Что включает в себя контекст потока?

a) Значения всех переменных программы

b) Состояние процессора и его регистров

c) Права доступа к устройствам

d) Приоритет задачи

24. Какая основная проблема возникает при не вытесняющей многозадачности?

a) Невозможность использовать многопоточность

b) Прерывания происходят в неподходящие моменты

c) Программист должен сам заботиться о передаче управления

d) Задачи выполняются дольше из-за накладных расходов

25. Какой механизм планирования характерен для дисциплины SRT?

a) Задачи выполняются в порядке их появления

b) Вытесняются задачи с наибольшим оставшимся временем выполнения

c) Вытесняются задачи с наименьшим временем до завершения

d) Задачи вытесняются на основе приоритета

26. Что происходит, если величина кванта времени в RR слишком велика?

a) Система тратит слишком много времени на переключения задач

b) Задачи могут долго ждать своей очереди на выполнение

c) Увеличивается количество прерываний

d) Система работает медленнее, но эффективнее

27. В чем отличие планировщика заданий от диспетчера задач?

a) Планировщик формирует очередь задач, а диспетчер

переключает процессор между ними

b) Диспетчер определяет приоритеты, а планировщик управляет памятью

c) Планировщик выполняет задачи, а диспетчер распределяет время процессора

d) Диспетчер завершает задачи, а планировщик их инициирует

28. В каких системах используется статическое планирование?

a) В универсальных операционных системах

b) В системах реального времени

c) В системах с заранее определенным набором задач

d) В системах с динамическими приоритетами

29. Какое из состояний относится к потоку?

a) Синхронизация

b) Ожидание

c) Остановка

d) Перемещение

30. Что такое диспетчеризация?

a) Управление контекстом процессов

b) Переключение процессора с одного потока на другой

c) Управление памятью процессов

d) Управление устройствами ввода-вывода

31. В чем особенность дисциплины диспетчеризации FCFS?

a) Каждая задача получает квант времени

b) Задачи выполняются в порядке их появления

c) Выполняется задача, которой осталось меньше всего времени

d) Используется динамический приоритет

32. Что характеризует дисциплину SJN?

a) Первым выполняется наиболее приоритетное задание

b) Первым выполняется задание, которому осталось меньше всего времени

c) Первым выполняется самое короткое задание

d) Каждой задаче выделяется квант времени

33. В чем особенность дисциплины RR?

a) Каждой задаче выделяется фиксированное время для выполнения

b) Задачи распределяются по приоритетам

c) Задачи обслуживаются в порядке их появления

d) Выполняется задача с наименьшим временем выполнения

34. Что такое вытесняющий алгоритм планирования?

a) Задача выполняется до завершения независимо от других

b) Задачи вытесняются операционной системой для выполнения других задач

c) Задача самостоятельно завершает выполнение перед переходом к следующей

d) Задача получает фиксированное время для выполнения

35. Какие задачи могут использоваться в статическом планировании?

a) Только задачи с неизвестным временем выполнения

b) Задачи, заранее известные системе

c) Все задачи без исключения

d) Задачи с динамическим приоритетом

Ключи к тестам

1) b

2) a

3) b

4) b

5) b

6) c

7) b

8) b

9) b

10) b

11) d

12) b

13) b

14) b

15) b

16) c

17) b

18) c

19) c

20) a

21) b

22) a

23) b

24) c

25) c

26) b

27) a

28) c

29) b

30) b

31) b

32) c

33) a

34) b

35) b

Критерии оценки

Процент результативности (правильных ответов)	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
30 - 35	5	отлично
25 - 29	4	хорошо
18 - 24	3	удовлетворительно
менее 18	2	неудовлетворительно

2. Задания промежуточной аттестации

Экзаменационные вопросы

Операционные системы для автономного компьютера

1. Понятие, назначение ОС. Основные функции операционных систем.

Архитектура операционной системы

2. Ядро и вспомогательные модули ОС.
3. Привилегированный, пользовательский режимы ОС.
4. Многослойная структура ОС, многослойная структура ядра ОС.

Процессы и потоки

5. Понятие «процесс» и «поток», состояния процесса.

6. Создание процессов и потоков, контекст процесса, дескриптор процесса.
7. Понятие планирования и диспетчеризации процессов.
8. Дисциплины диспетчеризации (понятие, примеры).
9. Понятие планирования. Планирование (статическое, динамическое).
10. Вытесняющие и не вытесняющие алгоритмы планирования.

Прерывания

11. Понятие прерывания. Назначение прерываний.
12. Механизм прерываний.
13. Виды прерываний.
14. Множественные (вложенные) прерывания.

Управление памятью

15. Функции ОС по управлению памятью. Типы адресов.
16. Страничное распределение памяти.
17. Сегментное распределение памяти.

Логическая организация файловой системы

18. Понятие файла, файловой системы. Цели и задачи файловой системы.
19. Типы файлов. Имена файлов. Атрибуты файлов, типы атрибутов.

Файловая система NTFS

20. Файловая система NTFS (особенности, цели, улучшения, недостатки).
21. Структура дискового тома под NTFS. Кластеры.
22. Главная файловая таблица MFT. Метафайлы.
23. Запись MFT (для файла, каталога). Резидентная, нерезидентная запись.
24. Файлы в системе NTFS. Структура файла MFT.
25. Атрибуты в NTFS. Резидентные и нерезидентные атрибуты.
26. Каталоги в NTFS. Структура каталога NTFS.

Безопасность в ОС

27. Понятие идентификации, аутентификации и авторизации.
28. Журнал аудита.
29. Программные и системные угрозы

Лист согласования к документу № 16 от 08.06.2026
Инициатор согласования: Фазылова А.А. Секретарь
Согласование инициировано: 08.06.2026 08:32

Лист согласования Тип согласования: **последовательное**

N°	ФИО	Срок согласования	Результат согласования	Замечания
1	Бикмухаметов З.М.		Подписано 08.06.2026 - 08:33	-