МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА–Российскийтехнологическийуниверситет» РТУ МИРЭА

Колледжпрограммирования икибербезопасности

Отчет о выполнении практического задания

по дисциплине «МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»

на тему «Аудит локальной системы»

Практическое задание № 13

Специальность–10.05.02 Информационная безопасность автоматизированных систем

Выполнил студент:

_____Маркаров М.О.

Группа: ИБ-32

Руководитель:

_____Герасин В.Ю.

Работа защищена с оценкой _____

Дата защиты _____

Москва

2025

Тема:Аудит локальной системы

Цель: приобретение обучаемыми необходимого объёма знаний и практических навыков в области настройки системы для задач аудита

Ход работы:

Задание 1. Произведите настройку аудита системы на своем ПК.

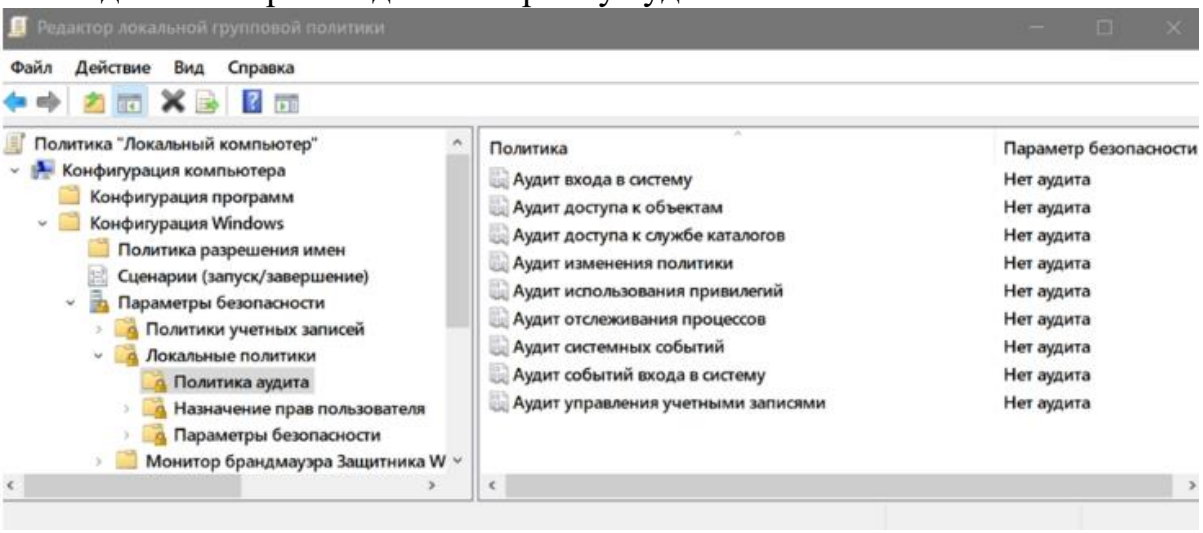

Рис. 1 Настройка аудита безопастности

Задание 2. Просмотреть события, происходящие в системе.

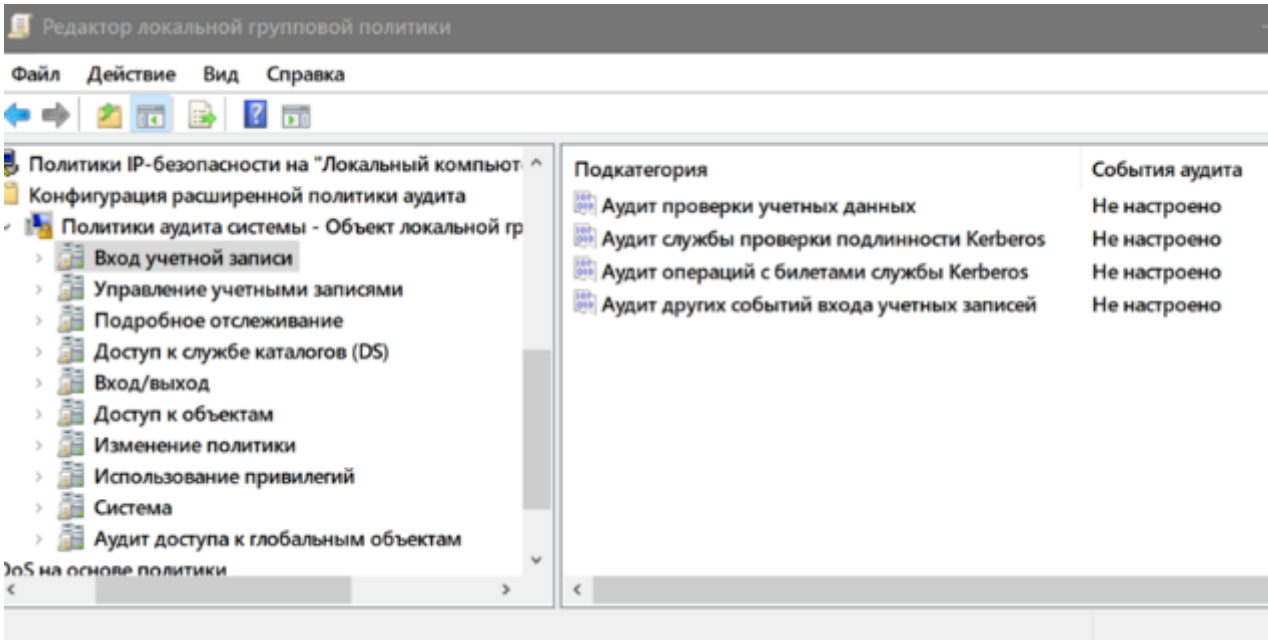

Рис. 2 Аудит событий безопасности ОС Windows

Для настройки событий откроем Политики аудита (Конфигурация компьютера / Конфигурация Windows / Параметры безопасности / Локальные политики / Политика аудита (Computer Configuration / Windows Settings / Security Settings / Local Policies / Audit Policy).

Задание 3. Проанализируйте текущие параметры системы.

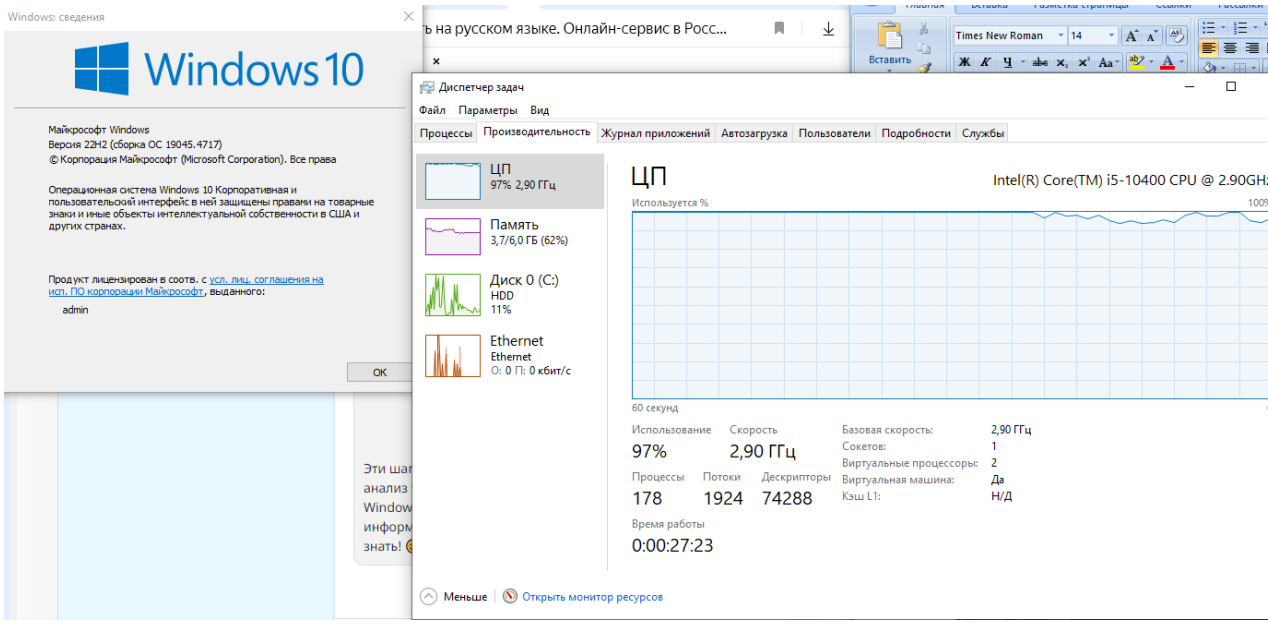

Рис. 3 Анализируйте текущие параметры системы

Задание 4. Просмотрите состояние сетевых соединений в Вашей системы.

Рис.4 Диагностика сетевых потоков с помощью команды netstat–a

На(рис.4) демонстрирует процесс показав сехактивных сетевых потоков.

Задание 5. Выполнить установку Secret Net Studio 8.9 (https://www.securitycode.ru/).

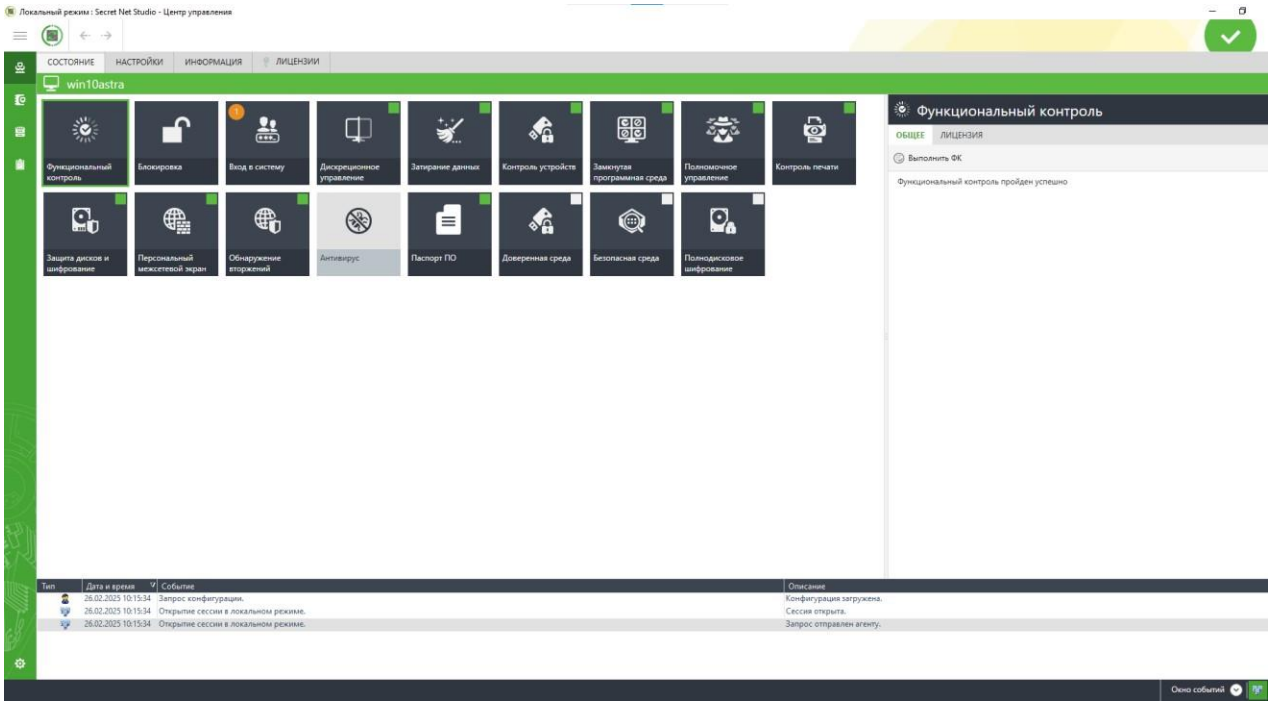

Рис.5 ПолноценноустановленнаяпрограммаSecretNetStudio

После настройки и вставления файла с электронной подписью для потвреждения что это не взломки мы использовали файл (Файл для установки Secret Net Studio 8 к заказу 000000111264D81B_key) далле будет установка на демонстрируется результат (рис. 5).

Задание 6. Настроить контроль печати конфиденциальных документов в Secret Net Studio.

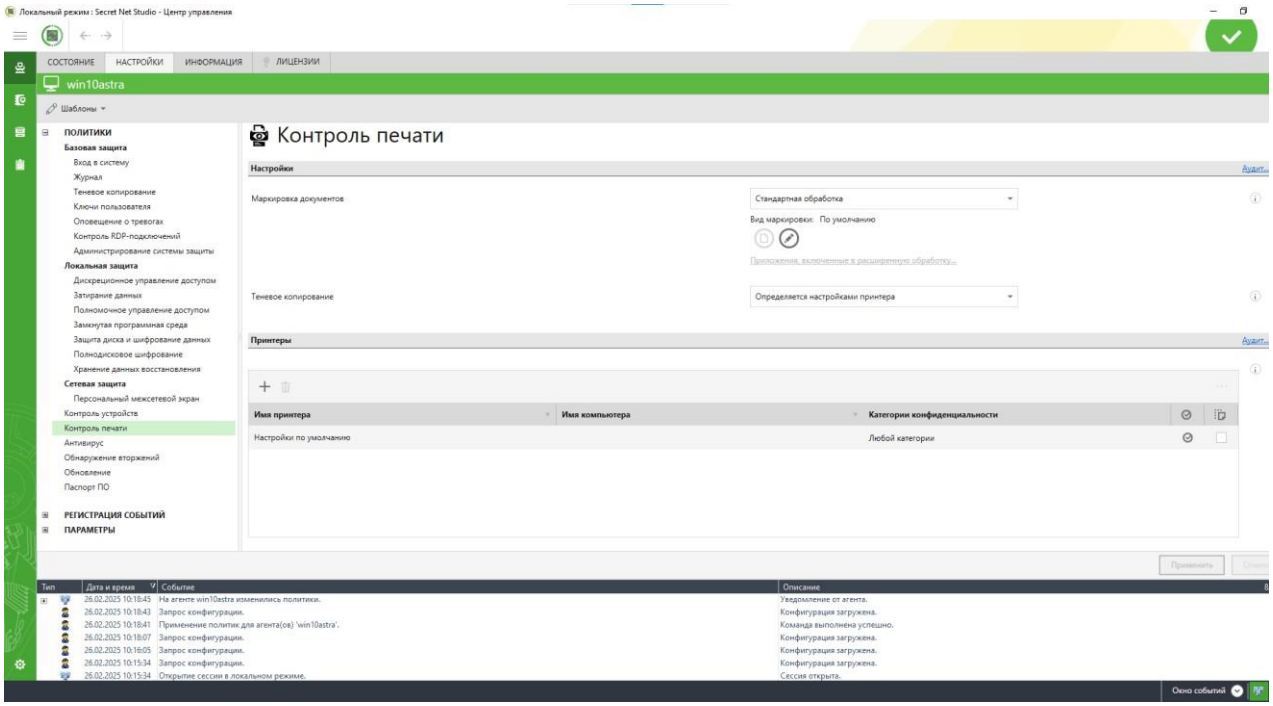

Рис.6 Настройка контроля печати

На (рис.6) демонстрируется результат выполнения настройки.

Теоретические вопросы:

Задание 1. Аудит событий. Настройка аудита событий.

Аудит событий - это процесс записи и мониторинга определенных действий, происходящих в операционной системе и приложениях. Эти действия регистрируются в журнале событий (event log) и могут включать в себя входы в систему, изменения файлов, доступ к ресурсам, запуск процессов и многое другое. Аудит событий используется для:

Обнаружения нарушений безопасности:Выявление несанкционированного доступа, попыток взлома или подозрительной активности.

Расследованияинцидентов:Сборинформациидляанализапричини последствий инцидентов безопасности.

Соответствиятребованиям:Подтверждениесоответствиянормативным требованиям и стандартам безопасности (например, GDPR, HIPAA).

Мониторингасистемы:Отслеживаниеработоспособностисистемыи выявление проблем.

Выявления проблем производительности: Анализ использования ресурсов и выявление узких мест.

Настройкааудитасобытий(Windows):

В Windows аудит событий настраивается через Редактор локальной групповой политики (gpedit.msc) илиРедактор групповой политики домена (GPMC). Основные шаги:

Запускредакторагрупповойполитики:

Нажмитеклавиши Win+R,введите gpedit.msc (длялокальной политики) или откройте GPMC (для доменной политики).

Переходкнастройкамаудита:

ПерейдитевразделКонфигурациякомпьютера->ПолитикиWindows->Параметрыбезопасности ->Локальныеполитики ->Аудит.(Computer Configuration-> Windows Settings -> SecuritySettings -> LocalPolicies -> Audit Policy)

Выборкатегорийаудита:

Выберитекатегориисобытий,которыевыхотитеотслеживать. Основныекатегории:

Auditaccountlogonevents (Аудитсобытийвходавучетнуюзапись) Audit

account management (Аудит управления учетными записями) Audit

directory service access (Аудит доступа к службе каталогов) Audit

logon events (Аудит событий входа)

Audit object access (Аудит доступа к объектам)

Auditpolicychange(Аудитизмененияполитик)

Audit privilege use (Аудит использования привилегий)

Auditprocesstracking(Аудитотслеживанияпроцессов) Audit

system events (Аудит системных событий)

Настройкарезультатоваудита:

Для каждой категории выберите, какие типы событий следует отслеживать:

Успех(Success): Записываетуспешныесобытия(например,успешный вход в систему).

Отказ(Failure):Записываетнеудачныесобытия(например,неудачная попытка входа в систему).

Можновыбратьобавариантa. Применение

политики:

После внесения изменений в политику необходимо обновитьгрупповыеполитики,выполнивкомандуgpupdate/forceвкоманднойстр окес правами администратора.

Дополнительныенастройки:

Расширенная настройка аудита:Для более детальной настройки аудита можно использовать Расширенную конфигурацию аудита безопасности (Advanced Audit Policy Configuration), расположенную вразделе Параметры безопасности. Она позволяет настраивать аудит для конкретных объектов (файлов, папок, ключей реестра) и категорий.

Размер журнала событий:Важно настроить размер журнала событий и параметры перезаписи, чтобы избежать его переполнения и потери данных. Это можно сделать через Просмотр событий (Event Viewer).

Сторонние инструменты:Существуют сторонние инструменты для аудита событий, которые предоставляют более широкие возможности для мониторинга и анализа.

Задание 2. Просмотр событий.

Просмотрсобытий(EventViewer)-этостандартноесредствоWindows

для просмотра журналов событий операционной системы и приложений. Он позволяет:

Просматривать журналы событий: Отображает события, зарегистрированные различными компонентами системы.

Фильтроватьсобытия:Позволяетфильтроватьсобытияпоразличным критериям (дата, время, источник, категория, уровень).

Поисксобытий:Позволяетискатьконкретныесобытияпоключевым словам.

Сохранять журналы событий:Позволяет сохранять журналы событий в различных форматах (EVTX, TXT, CSV).

Сортироватьсобытия: Позволяетсортироватьсобытияпоразличным столбцам (дата, время, источник, категория, уровень, пользователь).

Идентифицировать проблемы:Помогает выявлять проблемы в системе, приложениях и безопасности.

Какоткрытьпросмотрсобытий:

НажмитеклавишиWin+R,введитеeventvwr.mscинажмитеEnter. Найдите

“Просмотр событий” (Event Viewer) в меню “Пуск”.

Основныеразделыпросмотрщикасобытий:

Журналы Windows (Windows Logs): Содержит основные журналы событий системы:

Application (Приложение): Журнал событий, связанных с приложениями.

Security(Безопасность):Журналсобытий,связанныхсбезопасностью (например, входы в систему, изменения прав доступа).

Setup (Установка): Журнал событий, связанных с установкой и обновлением системы.

System(Система): Журнал событий, связанных с работой

операционнойсистемы.

Forwarded Events (Перенаправленные события): Журнал событий, полученных с других компьютеров (при настройке перенаправления событий).

Журналыприложенийслужб(ApplicationsandServices Logs):Содержит журналы событий, связанных с конкретнымиприложениями и службами.

Настраиваемые представления (Custom Views): Позволяет создавать пользовательские представления событий, отфильтрованные по определенным критериям.

Работаспросмотрщикомсобытий:

Выбор журнала событий:В левой панели выберите журнал, которыйвы хотите просмотреть.

Просмотр событий:События отображаются в центральной панели. Щелкните событие, чтобы увидеть подробную информацию о нем в нижней панели.

Фильтрациясобытий:

Нажмите “Фильтровать текущий журнал” (Filter Current Log) в правой панели.

Укажитекритериифильтрации(уровень,дата,время,источник,IDсобытия, ключевые слова, пользователь и т.д.).

Поисксобытий:

Нажмите“Найти”(Find)вправойпанели. Введите

ключевое слово для поиска.

Сохранениежурналасобытий:

Нажмите“Сохранитьвсесобытиякак…”(SaveAllEventsAs…)в правой панели.

Выберитеформатфайла(EVTX,TXT,CSV).

Диспетчерзадачивнутренниепараметрысистемы.

Диспетчер задач- это системная утилита Windows, предоставляющая информацию о работающих процессах, производительности системы, использовании ресурсов и сетевой активности. Он позволяет:

Просматривать запущенные процессы:Отображает список всех запущенных процессов, служб и приложений.

Завершать процессы:Принудительно завершать процессы, которые не отвечают или потребляют слишком много ресурсов.

Мониторить производительность системы: Отображает графики использования ЦП, памяти, диска и сети.

Управлять автозагрузкой:Отключать программы, автоматически запускающиеся при загрузке Windows.

Просматривать информацию о пользователях: Отображает список пользователей, вошедших в систему, и их ресурсы.

Анализировать использование ресурсов: Выявлять процессы, потребляющие больше всего ресурсов.

Какоткрытьдиспетчерзадач:

НажмитеклавишиCtrl+Shift+ Esc.

Нажмите клавишиCtrl + Alt + Deli выберите “Диспетчер задач” (Task Manager).

Щелкните правой кнопкой мыши по панели задач и выберите “Диспетчер задач” (Task Manager).

Вкладкидиспетчеразадач:

Процессы (Processes):Отображает список всех запущенных процессов, службиприложений,атакжеинформациюобиспользованииЦП,памяти,

дискаисетикаждымпроцессом.

Производительность (Performance): Отображает графики использования ЦП, памяти, диска, сети и GPU. Предоставляет информацию об общей загруженности системы.

Журнал приложений (App history): Отображает информацию об использовании ресурсов приложениями Microsoft Store.

Автозагрузка (Startup):Отображает список программ, автоматически запускающихся при загрузке Windows, и позволяет их отключать.

Пользователи (Users):Отображает список пользователей, вошедших в систему, и их ресурсы.

Подробности (Details):Отображает более подробную информацию о процессах, включая PID, приоритет, состояние и т.д.

Службы (Services):Отображает список служб Windows и позволяет их запускать, останавливать и перезапускать.

Внутренниепараметрысистемы:

Внутренние параметры системы включают в себя широкий спектр настроек, определяющих поведение и производительность операционной системы. Диспетчер задач предоставляет информацию о некоторых из этих параметров, но для доступа к более глубоким настройкам необходимо использовать другие инструменты:

Системные свойства (System Properties): Доступны через Win + Pause/Break или через “Панель управления” -> “Система и безопасность” -> “Система”. Позволяют настраивать:

Имя компьютера и рабочую группу.

Виртуальнуюпамять(размерфайлаподкачки).

Переменные среды.

Параметрызапускаивосстановления.

Производительность (визуальные эффекты, использование ЦП, памяти и диска).

Редактор реестра (Registry Editor - regedit.exe):Позволяет изменять параметры реестра Windows, которые определяют поведение операционной системы и приложений. Неправильное изменение реестра может привести к нестабильности системы, поэтому используйте этот инструмент с осторожностью.

Конфигурация системы (System Configuration - msconfig.exe): Позволяет настраивать параметры запуска, службы и автозагрузку.

Монитор ресурсов (Resource Monitor - resmon.exe):Предоставляетболее детальную информацию об использовании ЦП, памяти, диска и сети, чем диспетчер задач.

Производительность (Performance Monitor - perfmon.exe):Позволяет создавать графики производительности и мониторить различные системные счетчики.

Управление устройствами (Device Manager): Позволяет просматривать и управлять установленными устройствами, обновлять драйверы и устранять проблемы.

Задание 3. Проанализируйтетекущиепараметрысистемы

Диспетчера задач на внутренние параметры:

Диспетчер задач не изменяет напрямую большинство внутренних параметров системы. Он в основном используется для мониторинга и управления процессами и ресурсами. Однако:

Завершение процессов:Принудительное завершение процесса может повлиять на работу системы или приложения, если процесс был важным для его функционирования.

Отключениеавтозагрузки:Отключениепрограммизавтозагрузки

можетулучшитьскоростьзагрузкисистемы.

Мониторинг производительности: Информация, полученная из диспетчера задач, может помочь определить причины низкой производительности системы и принять меры для ее улучшения (например, увеличение объема памяти, замена жесткого диска на SSD).

Вывод: в этой работе мы применяли популярные команды в консоли linux использовали команды копирования архивирования и разархивирования.