Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МОНИТОРИНГ И УПРАВЛЕНИЕ СИСТЕМНЫМИ РЕСУРСАМИ

отчет о лабораторной работе №5

по дисциплине
ОПЕРАЦИОННЫЕ СИСТЕМЫ И ИХ БЕЗОПАСНОСТЬ

Выполнила:	студент гр. 230711	Павлова В.С.
Проверил:	доцент каф. ИБ	Антонов Д.М.

Тула, 2023 г

Лабораторная работа №5. Мониторинг и управление системными ресурсами

Введение

В этой лабораторной работе вы будете использовать административные инструменты для мониторинга и управления системными ресурсами.

Рекомендуемое оборудование

- Компьютер под управлением Windows с доступом в Интернет

Инструкции

Part 1: Просмотрщик событий

В этой части Защитник Windows используется для просмотра средства просмотра событий при изменении состояния службы. Защитник Windows — это встроенный в Windows компонент защиты от вредоносных программ.

Step 1: Убедитесь, что Защитник Windows запущен.

Примечание. Для работы Защитника Windows необходимо удалить с компьютера некоторые антивирусные и антишпионские программы.

a. Войдите в Windows как администратор.

b. Чтобы определить, остановлена ли служба Защитника Windows, нажмите кнопку **Пуск** и найдите **Защитник Windows**.

В Windows 10 щелкните **Защита от вирусов и угроз**. Прокрутите вниз до **настроек защиты от вирусов и угроз**. Щелкните **Управление настройками**. Под заголовком Защита в режиме реального времени убедитесь, что он **включен** .

В Windows 8.1 на вкладке **«Главная»** убедитесь, что защита в режиме реального времени включена . Если Защитник Windows не открывается, перейдите в **Центр поддержки** (нажмите **«Пуск»** > найдите **«Центр поддержки»** . Нажмите « **Включить сейчас»** для защиты от шпионских и нежелательных программ (важно) и защиты от вирусов (важно).

В Windows 7 вы получите сообщение **Эта программа отключена** в окне Защитника Windows. Щелкните **щелкните здесь, чтобы включить его** в окне, и щелкните **Закрыть** , чтобы продолжить.

c. Держите Защитник Windows открытым.

Step 2: Изучите консоль служб.

Примечание. Хотя большинством служб Windows можно управлять через консоль служб, остановить Защитника Windows из консоли **служб Windows** в Windows 10 и 8.1 невозможно.

a. Нажмите **«Пуск»** > найдите **«Панель управления»** . В Панели управления в представлении «Мелкие значки» нажмите **«Администрирование»** > нажмите **«Управление компьютером»** . В окне **«Управление компьютером»** разверните **«Службы и приложения»** и выберите **«Службы»** .

b. Прокрутите до окна «Управление компьютером» под заголовком «Службы», чтобы увидеть **службу проверки сети антивирусного защитника Windows** (Windows 10), **службу защитника Windows** (Windows 8.1) или **защитника окна** (Windows 7).

Вопрос:

В каком состоянии сервис?

Служба находится в состоянии «Выполняется».

c. Закройте окно **«Управление компьютером»**. Вернитесь к Защитнику Windows и выключите его.

В Windows 10 щелкните **Защита от вирусов и угроз** . Прокрутите вниз до **настроек защиты от вирусов и угроз** . Щелкните **Управление настройками** . Под заголовком Защита в режиме реального времени щелкните ползунок, чтобы отключить его. Нажмите **Да** чтобы разрешить этому приложению вносить изменения в устройство.

В Windows 8.1 на вкладке **«Параметры»** выберите вкладку **«Параметры»** . Во вкладке «Настройки» выберите **«Администратор»** . Щелкните **Включить это приложение** , чтобы отключить Защитник Windows. Нажмите **Сохранить изменения** , чтобы отключить Защитник Windows. При необходимости нажмите **«Закрыть»** во всплывающем окне.

В Windows 7 щелкните **Инструменты** . Щелкните **Параметры** . В окне «Параметры» выберите **«Администратор** » > нажмите **«Использовать эту программу»** . Нажмите **«Сохранить»** , чтобы остановить Защитник Windows. Нажмите **«Закрыть»** , чтобы продолжить, когда появится сообщение о том, что вы его отключили.

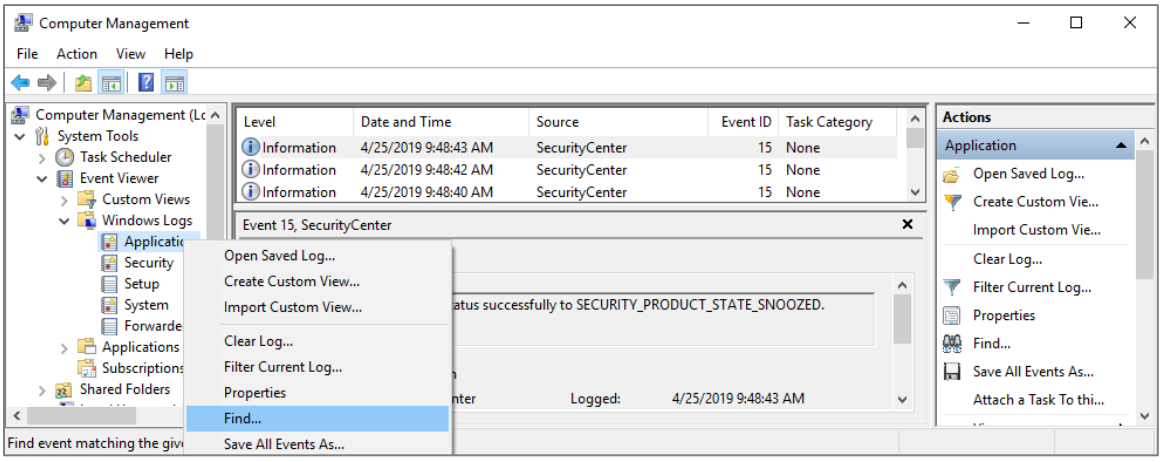
d. Вернитесь к Сервисам. (**Панель управления** в представлении «Мелкие значки» > **«Администрирование»** > **«Службы** »). Щелкните **Действие** > щелкните **Обновить** .

Найдите **Службу проверки антивирусной сети Защитника Windows** (Windows 10), **Службу Защитника Windows** (Windows 8.1) или **Защитник Windows** (Windows 7). Запишите статус Защитника Windows.

Теперь служба остановлена.

e. Перейдите к просмотрщику событий. В окне «Управление компьютером» разверните « **Системные инструменты** » > **«Просмотр событий** » > **«Журналы Windows »** > выберите **«Приложение»** (Windows 10), выберите **«Система»** (Windows 8.1 и 7).

f. На панели «Приложение» или «Система» вы можете найти самые последние события, связанные с Защитником Windows. Щелкните правой кнопкой мыши интересующий журнал и выберите **«Найти»**. Введите **защитник** для поиска записей, связанных с Защитником Windows.



На вкладке «Общие» что указано в качестве источника события? Каков уровень серьезности?

Состояние Windows Defender успешно изменено на SECURITY_PRODUCT_STATE_SNOOZED.

g. Перейдите к Защитнику Windows и включите его. Закройте Защитник Windows.

h. Перейдите к средству просмотра событий, чтобы просмотреть самые последние записи о событиях, связанных с Защитником Windows.

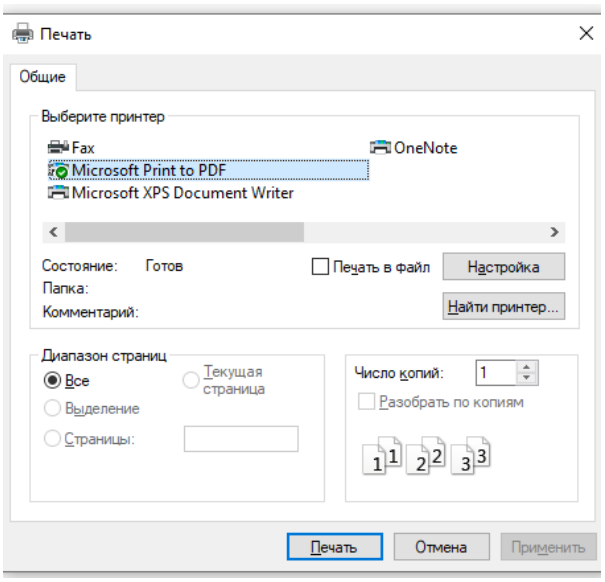
Part 2: Изучите влияние услуг.

В этой части вы остановите службу **диспетчера очереди печати**, чтобы исследовать влияние в системе. Диспетчер очереди печати отвечает за управление заданиями принтера и взаимодействие с принтером. Если эта служба отключена, вы не сможете печатать или видеть свои принтеры.

Step 1: Подтвердить услугу печати

a. Откройте **Блокнот**. Нажмите **«Пуск»** и найдите **«Блокнот»**.

b. В **Блокноте** щелкните **Файл** > **Печать**. Запишите принтер из списка ниже. **Примечание**. Вам не нужно устанавливать физический принтер.



c. Щелкните **Отмена**, чтобы выйти из диалогового окна печати.

Step 2: Остановить диспетчер очереди печати

a. Откройте консоль служб. (Панель управления > Администрирование > Службы)

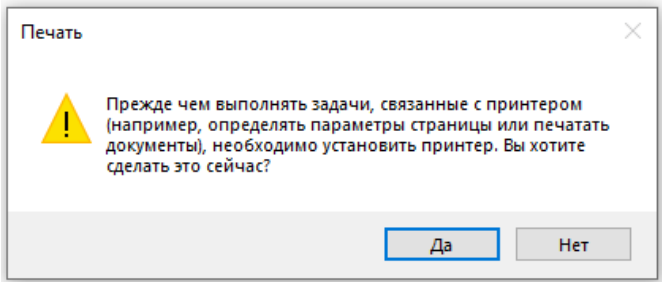
b. Щелкните правой кнопкой мыши **Диспетчер очереди печати** и выберите **Остановить**.

c. Перейдите в **Блокнот**. Попытка печати.

Вопрос:

Какое сообщение вы получили? Как бы вы это исправили?

Я полагаю, что необходимо включить диспетчер печати обратно.



d. Нажмите **«ОК»** или **«Нет»** в окне сообщения и нажмите «**Отмена»**, чтобы выйти из окна «Печать».

Step 3: Перезапустите диспетчер очереди печати

a. Перейдите к консоли **«Службы»** и перезапустите диспетчер очереди печати. Щелкните правой кнопкой мыши **Диспетчер очереди печати** и выберите **Пуск**.

b. Убедитесь, что вы можете печатать.

Step 4: Изучите службу DHCP-клиент

Служба DHCP-клиента регистрирует и обновляет IP-адреса и записи DNS для ПК. Если эта служба остановлена, ПК не получит динамический IP-адрес и обновления DNS.

a. В консоли служб найдите **DHCP-клиент.** Щелкните правой кнопкой мыши **DHCP-клиент** и выберите **Остановить**.

Вопрос:

Когда DHCP-клиент останавливается, какие другие службы также будут остановлены?

b. Нажмите **«Нет»** в окне **«Остановить другие службы»** .

Вопрос:

Почему важно проявлять осторожность при управлении услугами?

Осторожность при отключении каких-либо процессов в системе крайне необходима, поскольку можно случайно «зацепить» лишнее, что приведёт к ошибкам разного рода или потере какой-то информации, которая может быть важной.

c. Убедитесь, что **DHCP-клиент** все еще работает.

Part 3: Мониторинг и запись использования системы с помощью инструментов администрирования

Вы будете настраивать расширенные функции средства администрирования и контролировать использование системных ресурсов компьютера.

Step 1: Создайте новый набор сборщиков данных.

a. Перейдите в Панель управления> нажмите «Администрирование»> нажмите «Управление компьютером»> разверните «Инструменты системы».

b. Разверните **«Производительность»** > **«Наборы сборщиков данных»** > на левой панели щелкните правой кнопкой мыши « **Определено пользователем»** > выберите « **Создать»** > щелкните **«Набор сборщиков данных»** .

c. В окне **Создать новый набор сборщиков данных** введите **Журналы памяти** в поле Имя. Выберите **Создать вручную (Дополнительно)** и нажмите **Далее**, чтобы продолжить.

d. В поле «Какой тип данных вы хотите включить?» выберите Счетчик производительности и нажмите кнопку Далее.

e. В разделе **Какие счетчики производительности вы хотите регистрировать?** Окно, нажмите **Добавить** . В списке доступных счетчиков найдите и разверните **Память**. Выберите **«Доступные МБ» > «Добавить»** и нажмите **«ОК»** , чтобы продолжить.

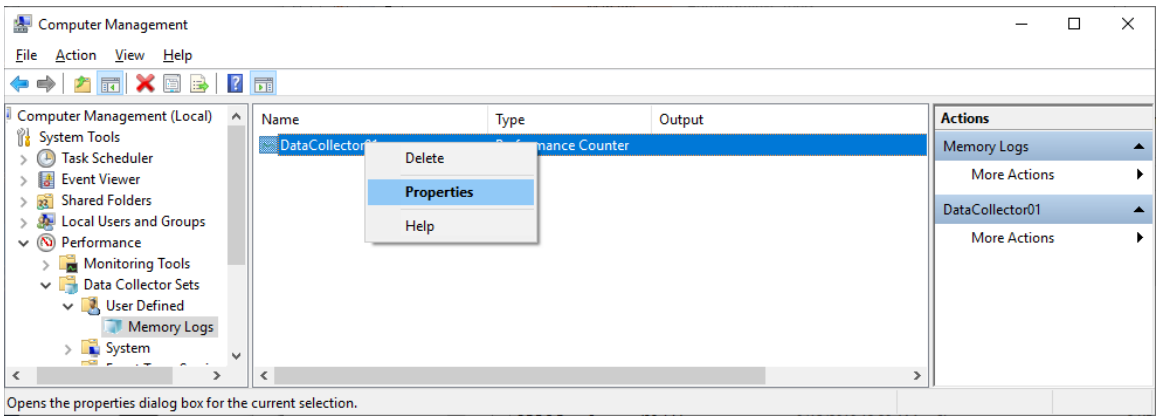
f. Установите в поле **Интервал выборки** : значение **4** секунды. Нажмите **Далее** , чтобы продолжить.

g. В разделе Где вы хотите сохранить данные? Окно, щелкните Обзор. Выберите Локальный диск (C:) и выберите PerfLogs . Нажмите OK, чтобы продолжить.

h. Убедитесь, что отображается правильный путь к корневому каталогу (C:\ PerfLogs), и нажмите **«Готово»** , чтобы продолжить.

Step 2: Отформатируйте набор сборщиков данных.

a. Разверните **«Определено пользователем»** и выберите **«Журналы памяти»** на левой панели. Щелкните правой кнопкой мыши **Data Collector01** и щелкните правой кнопкой мыши **Свойства** .



b. В окне свойств DataCollector01 измените формат журнала: на поле « **Разделенные запятыми»** .

c. Перейдите на вкладку **«Файл».**

Вопрос:

Каков полный путь к имени файла примера?

C:\PerfLogs\Admin\Журналы памяти\DESKTOP-RQFS0ST_20230319-000001\\Datacollector01.csv.

d. Нажмите **OK** , чтобы продолжить закрытие окна свойств.

Step 3: Собирайте и просматривайте данные.

a. Выберите значок **«Журналы памяти»** на левой панели окна **«Управление компьютером»** . Щелкните правой кнопкой мыши **«Журналы памяти»** и выберите **«Пуск»** .

b. Чтобы заставить компьютер использовать часть доступной памяти, откройте и закройте браузер.

c. Щелкните правой кнопкой мыши **«Журналы памяти»** и выберите **«Стоп»** , чтобы остановить сбор данных.

Перейдите к **Локальный диск (C:)\ PerfLogs** . Нажмите **«Продолжить»** в предупреждающих сообщениях Windows.

d. Откройте папку, созданную для хранения журнала памяти. Нажмите **«Продолжить»** в предупреждающих сообщениях Windows. Откройте файл **DataCollector01.csv** .

Выберите **Блокнот** или другую программу, которая может читать файлы с разделителями-запятыми (.csv), чтобы открыть файл, если Windows не может открыть файл, отображается сообщение.

Вопрос:

Что показывает крайний правый столбец?

e. Закройте файл DataCollector01.csv.

Step 4: Очистить

a. Перейдите в окно **«Управление компьютером»** . Выберите **«Производительность»** > щелкните **«Наборы сбора данных»** > щелкните **«Определено пользователем»** . Щелкните правой кнопкой мыши **Журналы памяти** и выберите **Удалить** . Нажмите **Да** , чтобы подтвердить удаление.

b. Перейдите на **локальный диск C: > папка PerfLogs** . Удалите папку сохраненных журналов памяти (папка с DataCollector01.csv), созданную из этой лабораторной работы.

c. Закройте все открытые окна.