ШИФР _____

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ТРУД (ТЕХНОЛОГИЯ)
2024/25 учебный год
МУНИЦИПАЛЬНЫЙ ЭТАП
ТЕОРЕТИЧЕСКИЙ ТУР
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ПРАКТИЧЕСКИЙ ТУР
10-11 классы

Уважаемый участник олимпиады!

Максимальная оценка – 35 баллов.

Продолжительность этапа – 180 минут

Для выполнения практического задания, необходимо наличие ПК, оснащенный процессором с поддержкой виртуализации, под управлением ОС Ubuntu (или другой ОС семейства Linux), с предустановленным программным обеспечением, необходимым для выполнения заданий (в зависимости от состава разработанных заданий).

Примерный состав ПО:

- средство виртуализации VirtualBox;
- среда разработки для языка программирования Python (Pycharm или аналог);
- анализатор сетевого трафика Wireshark;
- инструмент анализа памяти Volatility;
- платформа проведения аудита web-приложений BurpSuiteCommunityEdition;
- утилита strings;
- средство анализа образов носителей данных Mount;
- текстовый редактор;
- браузер Google Chrome.

Рекомендуемые минимальные системные требования:

- процессор с тактовой частотой не менее 3,2 ГГЦ;
- поддержка виртуализации или аналог,
- ОЗУ не менее 8 ГБ (желательно не менее 16 ГБ); свободное место на жестком диске не менее 256 ГБ

ШИФР _____

Практическое задание

Ваша компания обнаружила, что одно из ее устройств, которое используется для критически важных операций, стало работать медленнее и периодически отключаться. Вам поручили проанализировать дамп оперативной памяти (RAM) этого устройства, чтобы выявить возможные причины проблемы. Для этого вам потребуется использовать инструмент Volatility или другую подобную программу для анализа файлов формата mem или иных форматов дампа оперативной памяти.

Анализ использования памяти:

- Проанализируйте использование памяти в оперативной памяти.
- Проверьте, есть ли процессы, которые потребляют неоправданно много памяти.

Анализ дефектных страниц:

- Просмотрите список дефектных страниц и поврежденных участков памяти.
- Проверьте, связаны ли эти дефекты с известными ошибками или вредоносной активностью.

Создание отчета:

- Соберите все результаты анализа в единый отчет.
- Опишите найденные проблемы с использованием ресурсов процессора и памяти.
- Дайте рекомендации по устранению возможных угроз и оптимизации работы устройства.

Ответьте на вопросы:

1. Какие процессы занимают больше всего ресурсов процессора?
2. Есть ли процессы, которые потребляют неоправданно много памяти?
3. Есть ли дефектные страницы или поврежденные участки памяти?
4. Связаны ли эти дефекты с известными ошибками или вредоносной активностью?
5. Какие рекомендации по устранению проблем и оптимизации работы устройства вы можете дать?

ШИФР _____

Карта пооперационного контроля для участников и жюри по профилю

«Информационная безопасность»

№ п/п	Критерии оценивания	Макс. балл	Кол-во баллов, выставленных членами жюри		
1.	Школьник открыл информацию об оперативной памяти	3			
2.	Найдена информация в процентном соотношении о потреблении памяти на пк	3			
3.	Оформлен отчёт в формате документа	4			
4.	Описаны проблемы с использованием ресурсов процессора и памяти	5			
5.	Прописаны рекомендации по устранению возможных угроз и оптимизации работы устройства	5			
6.	Найдены ответы на вопросы	3x5			
	Итого:	35			

Ключи

По практическому туру максимальная оценка результатов участника возрастной группы (10-11 классы) определяется арифметической суммой всех баллов, полученных за выполнение заданий и не должна превышать 35 баллов.

Задание

1. Открыть «Диспетчер задач» (Ctrl + Shift + Esc).
2. Перейти на вкладку «Процессы».
3. Нажать на заголовок столбца «CPU», чтобы отсортировать процессы в зависимости от их загрузки процессора.
4. Составить отчёт

   Ответы на вопросы

- Какие процессы занимают больше всего ресурсов процессора?

Вредоносные программы и вирусы

Фоновые процессы и службы. Некоторые законные фоновые процессы, например поиск в Windows или сканирование Защитником Windows, могут потреблять значительные ресурсы процессора.

Устаревшие или несовместимые драйверы устройств.

Нехватка системных ресурсов. Например, низкий объём оперативной памяти может вызвать нагрузку на процессор.

Программные конфликты и сбои. Нужно проверить, нет ли недавно установленных программ или обновлений, которые могут вызывать проблему

- Есть ли процессы, которые потребляют неоправданно много памяти?

Svchost.exe и служба wuauserv. Стандартная служба обновления Windows сканирует компьютер, ищет, закачивает и устанавливает новые обновления. Из-за проблем в коде служба может потреблять всю доступную ей память вплоть до 1,5–2 Гб

- Есть ли дефектные страницы или поврежденные участки памяти?

Дефектные страницы или повреждённые участки памяти — это разные понятия.

Дефектные страницы — это блоки чтения/записи, не поддающиеся записи и стиранию. Например, в flash-памяти к ним относятся блоки, которые содержат записанные данные и принадлежат какому-либо файлу.

Повреждённые участки памяти — это, например, случаи, когда драйвер или устройство неправильно изменяет физические страницы, или когда оборудование оперативной памяти неисправно.

Для диагностики повреждений памяти можно использовать, например, средство диагностики памяти Windows. Чтобы его запустить, нужно ввести «Память» в поле поиска панели управления, а затем выбрать «Диагностика проблем с памятью компьютера». После выполнения теста результаты можно посмотреть в системном журнале.

- Связаны ли эти дефекты с известными ошибками или вредоносной активностью?

Да, дефектные страницы и повреждённые участки памяти могут быть связаны с известными ошибками и вредоносной активностью

- Какие рекомендации по устранению проблем и оптимизации работы устройства вы можете дать?

Проверка установленных приложений. Нужно перейти в настройки, открыть раздел «Приложения» и удалить те, которые не используются. Это освободит место и улучшит производительность устройства.

Очистка кэша приложений. Некоторые приложения накапливают кэш, который может занимать значительное количество памяти. Очистить кэш можно через настройки.

Удаление ненужных файлов. Для этого можно использовать встроенные инструменты для очистки памяти или сторонние приложения. Например, старые фотографии, видео и документы.

Управление автозапуском приложений. В настройках устройства нужно найти раздел «Автозапуск приложений» и отключить автозапуск для тех приложений, которые не нужны сразу после включения устройства.

Настройка анимаций и визуальных эффектов. Анимации и визуальные эффекты могут замедлять работу устройства. Отключение или уменьшение анимаций поможет улучшить производительность.

Оптимизация настроек сети. Если не используются Bluetooth, NFC или Wi-Fi, их нужно отключить, чтобы снизить нагрузку на устройство.

Регулярное обновление системы и приложений. Обновления системы и приложений часто включают исправления ошибок и улучшения производительности.

Обеспечение безопасности устройства. Нужно установить антивирусное приложение, которое будет сканировать устройство на наличие вредоносных программ и защищать его.

Регулярная перезагрузка устройства. Это помогает очистить оперативную память и завершить ненужные процессы