Лабораторная работа 11
Использование штатных средств защиты операционной системы и прикладных программ.

1. Цель работы:
1.1 Научиться защищать ОС Windows 10-11.

2. Литература:

3. Оборудование
3.1 Персональный компьютер
3.2 Программа LibreOffice Writer

4. Подготовка к работе
4.1 Ознакомится с приложением

5. Задание
5.1 Проверка состояния защиты
- Откройте Защитник Windows (через Параметры → Обновление и безопасность → Безопасность Windows).
- Проверьте, включены ли:
- Защита от вирусов и угроз
- Защита учетных записей
- Брандмауэр и безопасность сети
- Сделайте скриншот и объясните, что означает каждый пункт.

5.2 Быстрое сканирование
- Запустите быстрое сканирование на наличие угроз.
- Дождитесь завершения, сохраните отчет (можно через PowerShell: Get-MpThreatDetection).
- Определите, какие файлы были проверены, и были ли найдены угрозы.

5.3 Обновление антивирусных баз
- Вручную проверьте актуальность сигнатур вирусов.
- Запустите обновление через Центр обновления Windows или вручную через PowerShell (Update-MpSignature).
- Запишите, какая версия баз установлена (можно найти в журнале Защитника).

5.4 Полное сканирование и карантин
- Запустите полное сканирование системы.
- Если найдены подозрительные файлы, переместите их в карантин.
- Изучите журнал событий Защитника (Event Viewer → Applications and Services Logs → Microsoft → Windows → Windows Defender).

5.5 Настройка исключений

- Создайте тестовый файл (например, test.txt).
- Добавьте его в исключения Защитника, чтобы он не проверялся.
- Проверьте, работает ли исключение, попытавшись просканировать файл.

5.6 Анализ работы в PowerShell

- Используйте PowerShell для проверки статуса Защитника:

```
Get-MpComputerStatus
```

- Определите, когда было последнее сканирование, включена ли защита в реальном времени.
- Выведите список последних угроз (Get-MpThreat).

5.7 Тестирование реакции на угрозу

- Скачайте тестовый вирус (EICAR – безопасный тестовый файл: X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*).
- Сохраните его на компьютер и проверьте, как Защитник отреагирует.
- Проанализируйте, в какой момент сработала защита (при скачивании, открытии и т. д.).

5.8 Сравнение с другими антивирусами

- Установите бесплатный антивирус (например, Kaspersky Free).
- Проведите тестовое сканирование и сравните результаты с Защитником.
- Определите плюсы и минусы каждого.

6 Порядок выполнения работы

6.1 Ознакомится с приложением

6.2 Выполнить задания из пункта 5. Ответы занести в отчёт.

6.3 Ответить на контрольные вопросы.

7 Содержание отчета

7.1 Выполненные задания из пункта 5.

8 Контрольные вопросы

8.1 Что такое windows defender?

8.2 Что такое сканирование системы?