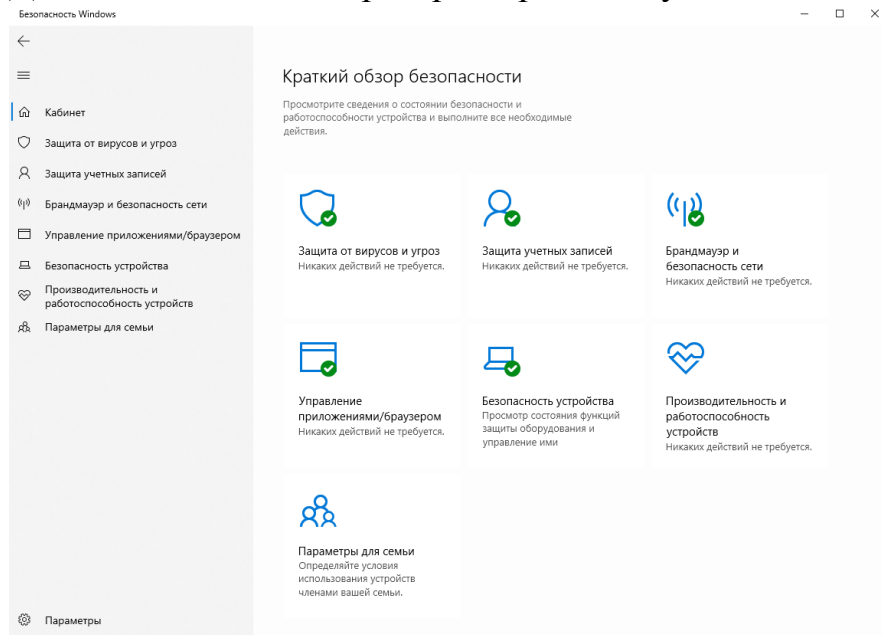


Для выполнения Лабораторной работы будет использован антивирус Windows.



Задание 1: Результаты сканирования диска и дискеты запишите в отчёт.  
Результат сканирования диска D:

## Параметры сканирования

Выполнить быстрое, полное, специальное сканирование или сканирование Автономным модулем Microsoft Defender.

Текущих угроз нет.

Последнее сканирование: 03.12.2021 18:21 (настраиваемая проверка)

Найдены угрозы (0).

Проверка длилась 25 мин 58 с

Проверено файлов: 3267524.

[Разрешенные угрозы](#)

[Журнал защиты](#)

Задание 2: В разделе Справочной системы программы найдите информацию о том, какие три уровня очистки поддерживает программа и запишите эту информацию в отчёт.

Уровень очистки	Описание
Всегда исправлять обнаружения	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, с системными файлами), если обнаружение не удастся исправить, обнаруженный объект оставляется в исходном расположении. Функция <b>Всегда исправлять обнаружения</b> является рекомендуемой настройкой.
Исправлять обнаружения, если это безопасно, в другом случае оставить	Пытаться исправлять обнаружения при очистке объектов без вмешательства конечного пользователя. В некоторых случаях (например, системные файлы или архивы, которые содержат и чистые, и зараженные файлы), если обнаружение не удастся исправить, обнаруженный объект остается в исходном расположении.
Исправлять обнаружения, если это безопасно, в другом случае спрашивать	Пытаться исправлять обнаружения при очистке объектов. В некоторых случаях, если ни одно из действий выполнить невозможно, конечный пользователь получает интерактивное предупреждение, в котором следует выбрать действие по исправлению (например, удалить или проигнорировать). Этот параметр рекомендуется в большинстве случаев.
Всегда спрашивать у конечного пользователя	Конечному пользователю отображается интерактивное окно при очистке объектов, и он должен выбрать действие по исправлению (например, удалить или пропустить). Этот уровень предназначен для более опытных пользователей, которые знают, какие действия следует предпринять в случае обнаружения.

### Задание 3: Изучите раздел справки Предупреждения и уведомления.

#### Уведомления

Функция "Безопасность Windows" будет отправлять уведомления с критически важными сведениями о работоспособности и безопасности вашего устройства. Вы можете указать, какие информационные уведомления хотите получать.

#### Уведомления о защите от вирусов и угроз

Получать информационные уведомления



Вкл.

- ☒ Последние действия и результаты сканирования
- ☒ Найдены угрозы, но немедленные действия не требуются
- ☒ Файлы или действия заблокированы

[Параметры защиты от вирусов и угроз](#)

#### Уведомления о защите учетной записи

Получение уведомлений о защите учетной записи



Вкл.

- ☒ Проблемы с Windows Hello
- ☒ Проблемы с динамической блокировкой

#### Уведомления от функции "Брандмауэр и защита сети"





Уведомлять, когда брандмауэр Microsoft Defender блокирует новое приложение



Вкл.

- ☒ Брандмауэр домена
- ☒ Частный брандмауэр
- ☒ Общественный брандмауэр

### Задание 4: В служебных программах в Планировщике почитайте, какие задачи запланированы на ближайшее время и запишите эту информацию в отчёт.

Файл	Состояние	Триггеры	Время следующего запуска	Время прошлого запуска	Результат последнего запуска	Автор	Создан
 Windows De...	Готово			02.12.2021 18:39:29	Операция успешно завершена. (0x0)		
 Windows De...	Готово			02.12.2021 18:39:29	Операция успешно завершена. (0x0)		
 Windows De...	Готово			02.12.2021 18:39:09	(0x2)		
 Windows De...	Готово			02.12.2021 18:39:29	Операция успешно завершена. (0x0)		

#### Контрольные вопросы.

##### 1. Что такое вирус?

Вирус — это часть программного кода, которая тиражируется путем добавления в другой объект, обычно незаметно и без разрешения пользователя.

##### 2. Какие разновидности вирусов Вы знаете?

- Троянский конь

- Черви
- Логические бомбы
- Смешанные коды

3. Как вирусы классифицируются по среде обитания?

- Загрузочный сектор
- Файловые
- Макровирусы

4. Как вирусы классифицируются по степени вредного воздействия?

Вирусы могут быть безвредными, малоопасными и разрушительными.

5. Какие виды вредоносных программ Вы знаете?

- вирусы
- макровирусы для Word и Excel
- загрузочные вирусы
- скрипт-вирусы, включая batch-вирусы, заражающие оболочку ОС Windows, Java-приложения и т.д
- клавиатурные шпионы
- программы для кражи паролей
- троянцы-бэкдоры
- crimeware — вредоносные программы, созданные для автоматизации совершения финансовых преступлений
- шпионские программы
- рекламные программы и другие типы вредоносных программ

6. Как вирусы маскируются?

Вирусы-невидимки скрывают изменения, вносимые в размер файлов, структур каталогов или иных разделы операционной системы.

Зашифрованные вирусы во время работы шифруют свой вирусный код.

Полиморфные вирусы могут изменять свой внешний вид при каждом инфицировании.

Многокомпонентные вирусы инфицируют как загрузочные секторы, так и исполняемые файлы.

Самообновляющиеся вирусы способны скрытно обновляться через Интернет во время сеансов связи.

7. Когда обнаружили первый вирус?

Официальное появление первого компьютерного вируса датируется 1981 годом, за-долго до выхода первой версии Microsoft Windows.

8. Как Вы думаете, зачем изобретают вирусы?

Для получения доступа к личным данным других пользователей.

9. Какие действия могут выполнять антивирусные программы?

- Сканирование цифровой сигнатуры
- Эвристический анализ
- Исследование памяти
- Мониторинг прерываний
- Контроль целостности

10. Какие три задачи должна выполнять антивирусная программа?

- Обнаружение вируса
- Удаление вируса

- Защита от вирусов

#### 11. Как обеспечить безопасность своей информации?

Установить и настроить антивирусную программу, блокировать рассылку реклам с различных сайтов, быть бдительными и аккуратными при переходе на незнакомые ссылки и скачивании/открытии файлов, использовать источники информации о компьютерных вирусах и «ложных тревогах», пользоваться программами для резервного копирования.