|  |
| --- |
| 4.1. Защита на устройства  Интерактивна демонстрация  Защита на системата/ БЕЗОПАСТНОСТ – БАЗОВО НИВО |
|  |
| Съдържание  [1 Интерактивна демонстрация за защита на системата 1](#_Toc127960031)  [1.1 Защита на системата в Windows 1](#_Toc127960032)  [1.2 Възможности за защита 1](#_Toc127960033)  [1.3 Проверка на сигурността на системата 2](#_Toc127960034)  [1.4 Защита от вируси и заплахи 3](#_Toc127960035)  [1.4.1 Текущи заплахи 4](#_Toc127960036)  [1.4.2 Видове сканирания 4](#_Toc127960037)  [1.5 Защита на устройството с най-новите актуализации 7](#_Toc127960038)  [1.6 Ръчно изпълнение на сканиране за злонамерен софтуер 9](#_Toc127960039)  [1.7 Включване или изключване на защитата Microsoft Defender Antivirus 9](#_Toc127960040)  [1.8 Деинсталиране на антивирусен софтуер 10](#_Toc127960041)  [1.9 Използвана литература 11](#_Toc127960042) |

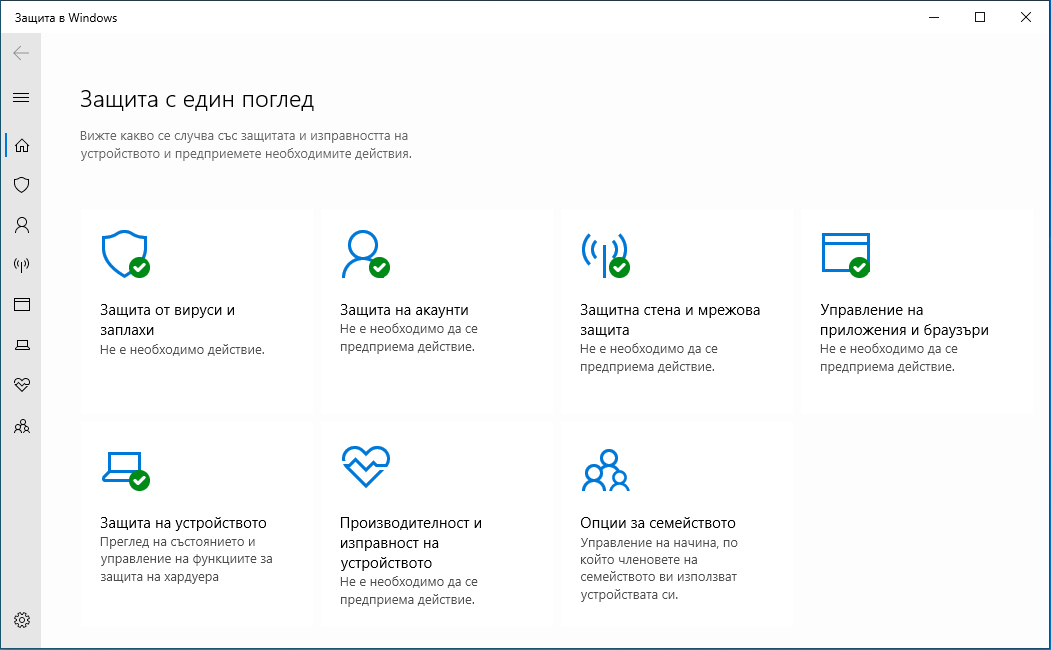
# Интерактивна демонстрация за защита на системата

## Защита на системата в Windows

Windows включва вградена защита (Windows Security), която съдържа най-новата антивирусна програма - Microsoft Defender Antivirus. (Фигура 1)

Устройство с Windows e активно защитено от момента, в който се стартира системата и не е необходима отделна инсталация на антивирусен софтуер.

Сканиране за злонамерен софтуер, вируси и заплахи за защитата се извършва непрекъснато. В допълнение към тази защита в реално време, актуализациите се изтеглят автоматично, за да помагат за защитата на устройство и да го защитават от заплахи.



Фигура 1. Защита в Windows (Windows Security)

За да управлявате инструментите, които защитават вашето устройство и вашите данни, отворете Windows Security, като изберете Старт бутона (Start) -> Настройки (Settings) -> Актуализиране и Защита (Update & Security) - > Защита в Windows (Windows Security)



## Възможности за защита

От основния прозорец ще видите следните възможности за защита:

* Защита от вируси и заплахи – Проследяване за заплахи на устройството, извършване на сканирания и получаване актуализации, с които да се откриват най-новите заплахи.
* Защита на акаунти – Достъп до опциите за влизане и настройките на потребителския акаунт.
* Защитна стена и мрежова защита – Възможност за управление и настройка на защитната стена, както и наблюдение какво се случва с мрежите и интернет връзките.
* Управление на приложения и браузъри – Възможност за актуализиране на настройките за защита на устройството от потенциално опасни приложения, файлове, сайтове и изтегляния (Microsoft Defender SmartScreen). Може да се персонализират настройките за защита за устройствата чрез Exploit Protection.
* Защита на устройството – Преглеждане на вградените опции за защита, за защита на устройството от атаки със злонамерен софтуер.
* Производителност и изправност на устройството – Преглеждане на информацията за състоянието на изправността на производителността на устройството и поддържане на устройство изчистено и актуализирано с най-новата версия на Windows.
* Опции за семейството – Проследяване на онлайн дейността на децата и на устройства в дома.

## Проверка на сигурността на системата

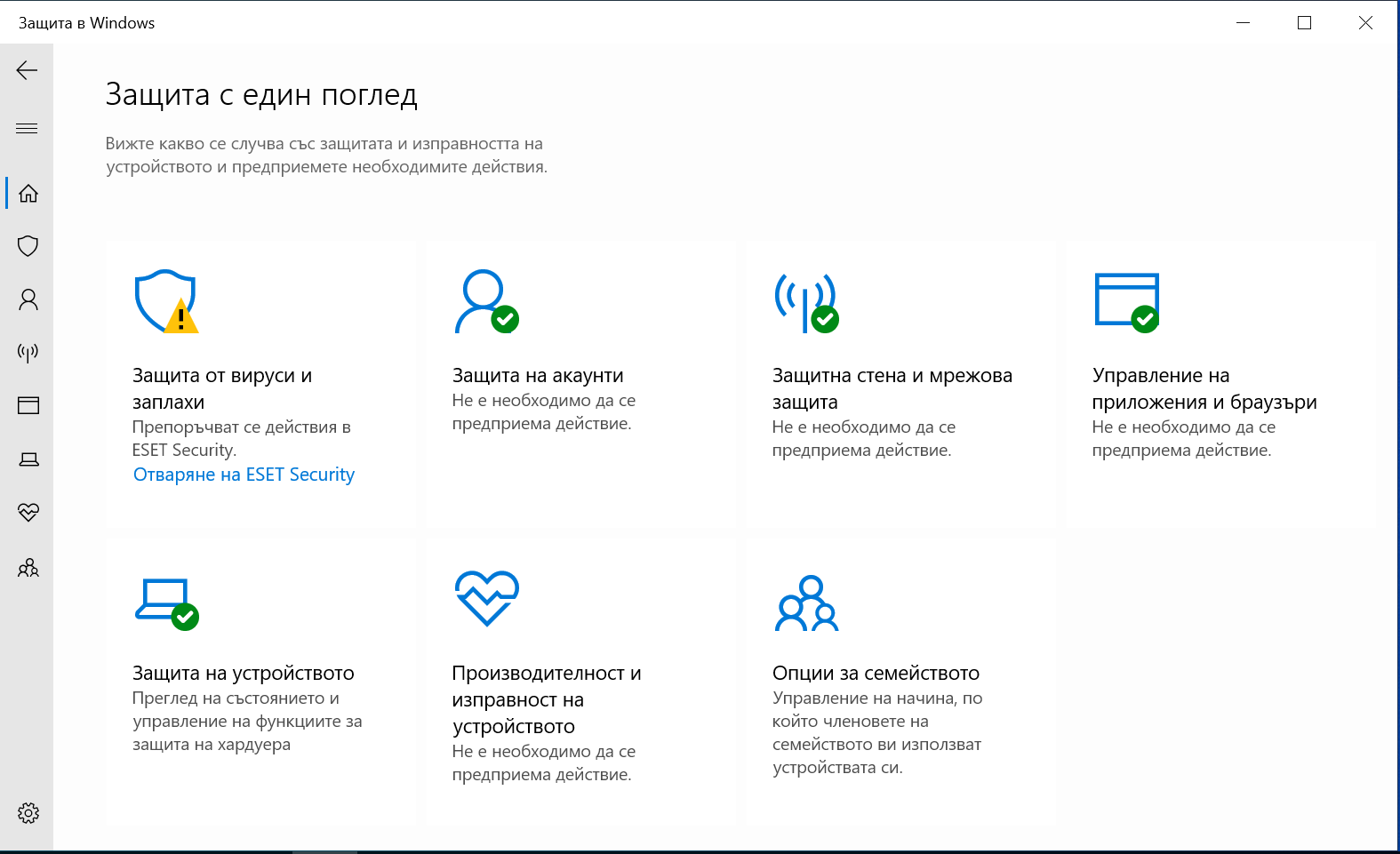
Статусът за защитата на системата можете да видите от основния прозорец на Windows Security.

За състоянието на вашето ниво на защита, се използват следните икони:

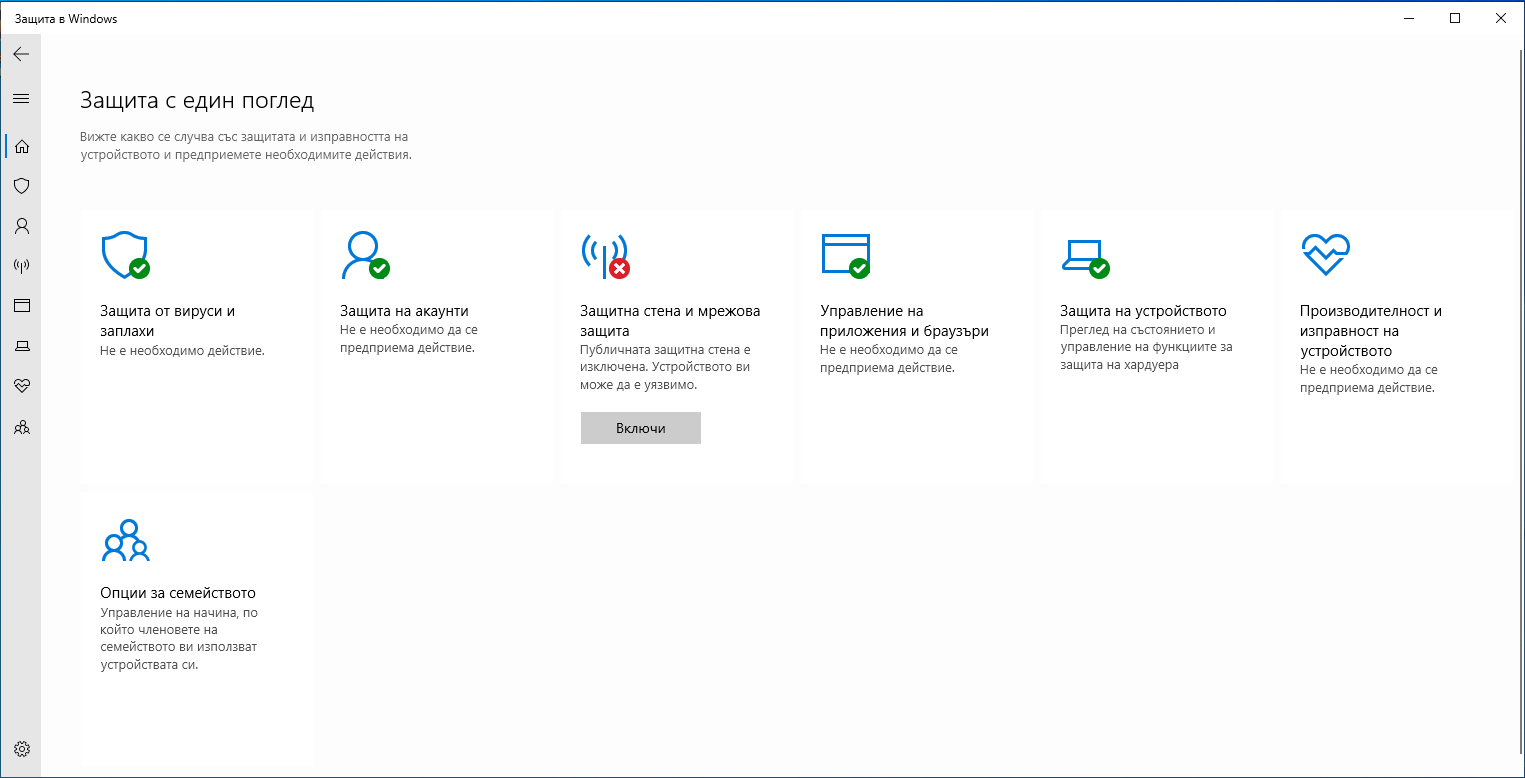
* **Зеленото** означава, че в момента няма препоръчителни действия.

(Фигура 1)

* **Жълтото** означава, че има препоръка за безопасност за вас. (Фигура 2)
* **Червеното** е предупреждение, че нещо изисква вашето незабавно внимание. (Фигура 3)



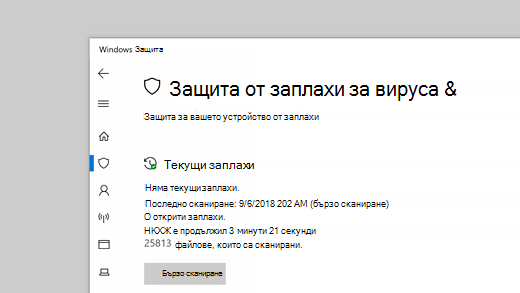
Фигура 2. Windows Defender с препоръка за безопасност



Фигура 3. Windows Defender с предупреждение за незабавно внимание

## Защита от вируси и заплахи

**Защита от вируси и заплахи** в "Защита в Windows" (Windows Security) Ви помага да сканирате за заплахи на вашето устройство. Можете също да изпълнявате различни типове сканирания, да виждате резултатите от предишните сканирания на вируси и заплахи и да получите най-новата защита, предлагана от Microsoft Defender Antivirus. (Фигура 4).



Фигура 4.Windows Security - Защита от вируси и заплахи

### Текущи заплахи

Под Текущи заплахи (Current threats) можете да: (Фигура 8)

* Видите всички заплахи, които в момента са открити на вашето устройство.
* Видите последния път, когато е изпълнено сканиране на Вашето устройство, колко време е отнело и колко на брой файла са сканирани.
* Започнете ново бързо сканиране или отидете в опции за сканиране, за да изпълните по-обширно или персонализирано сканиране.
* Видите заплахите, които са поставени под карантина, преди да могат да ви засегнат и всичко, идентифицирано като заплаха, която сте разрешили да се изпълнява на вашето устройство.

*Трябва да знаете, че ако сте инсталирали и включили друго антивирусно приложение, Microsoft Defender Antivirus ще се изключи автоматично и Вие ще можете да използвате опциите за защита от вируси и заплахи на другото антивирусно приложение. Ако деинсталирате другото приложение, тогава Microsoft Defender Antivirus ще се включи отново автоматично.*

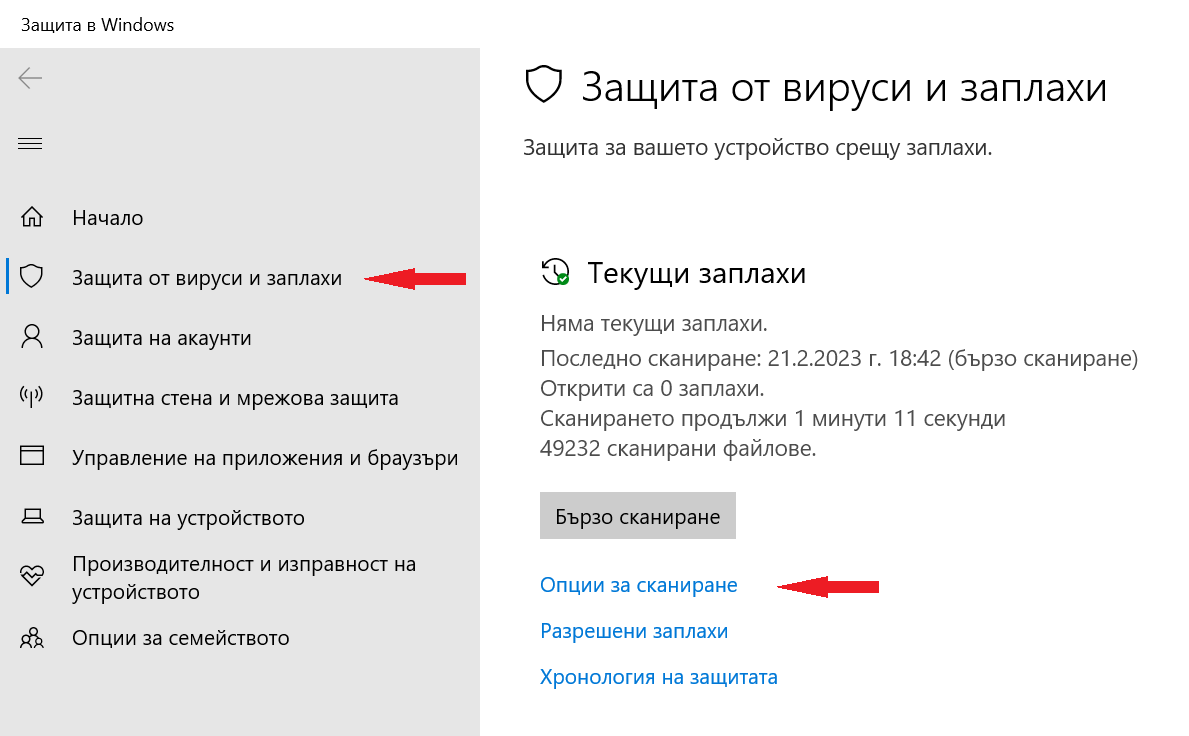
### Видове сканирания

Въпреки че „Windows Security” е включена и автоматично сканира вашето устройство, можете да изпълните допълнително сканиране всеки път, когато искате.

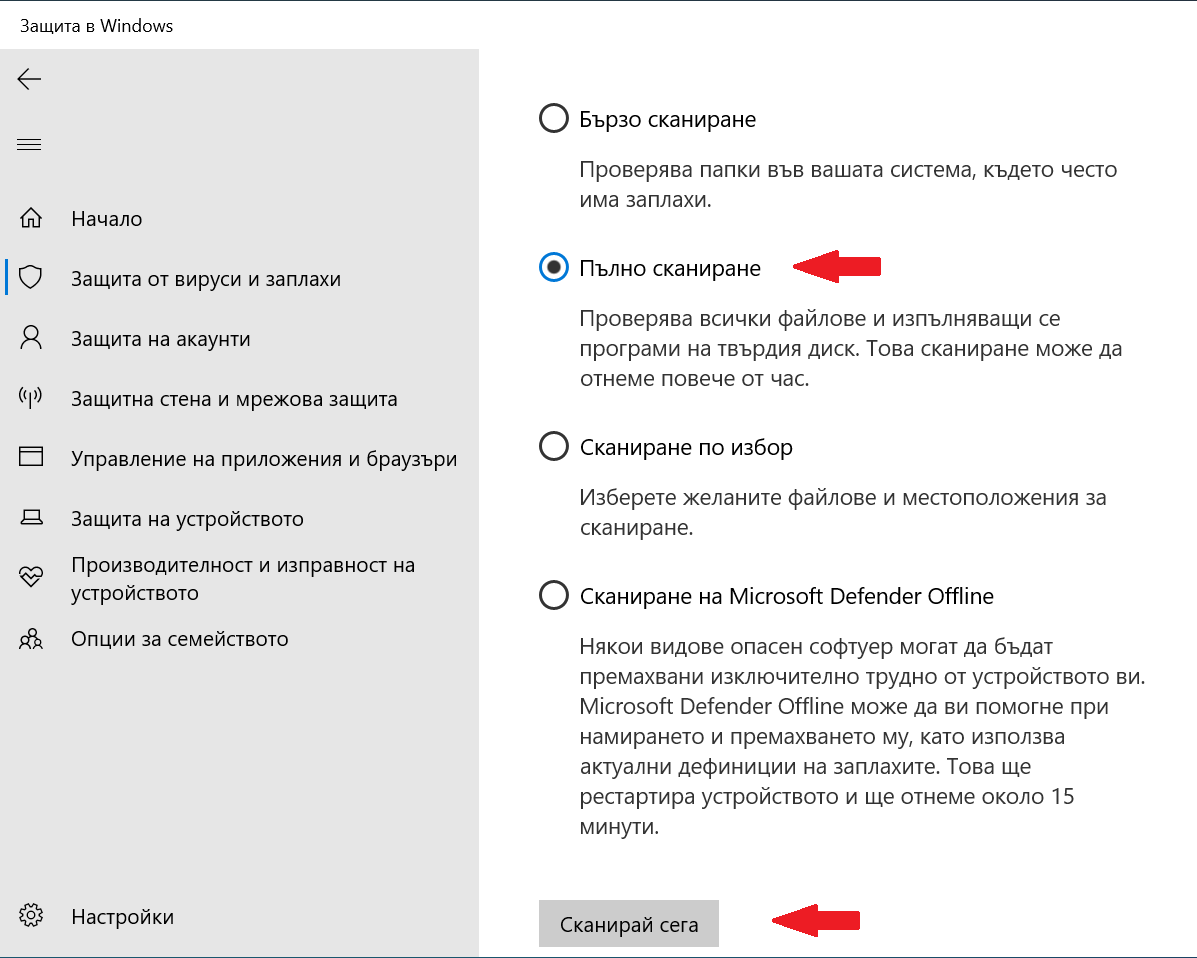
* **Бързо сканиране (Quick scan)** - Незабавна проверка на вашето устройство за всякакви скорошни заплахи. Тази опция е полезна, когато не искате да губите време с изпълнението на пълно сканиране на всички ваши файлове и папки.

Ако "Windows Security " ви препоръчва да изпълните един от другите типове сканирания, ще бъдете уведомени, когато бързото сканиране приключи.

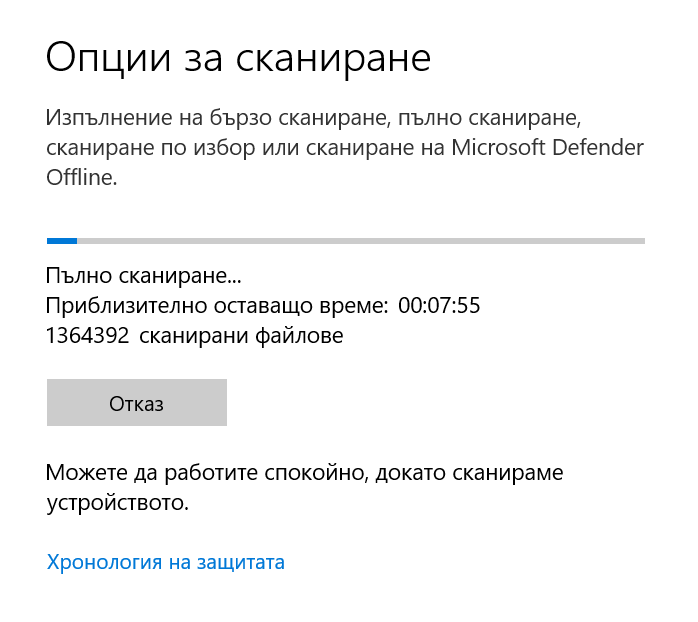
* **Опции за сканиране (Scan options)** – дава възможност за един от следните разширени опции за сканиране: (Фигура 5)
  + **Пълно сканиране (Full scan)** - Сканира всеки файл и програма на Вашето устройство. (Фигура 6), (Фигура 7)
  + **Сканиране по избор (Custom scan)** - Сканира само файлове и папки, които сте избрали.
  + **Microsoft Defender Офлайн сканиране (Microsoft Defender Offline scan)** - Използва най-новите дефиниции за сканиране на вашето устройство за най-новите заплахи. Това се случва след рестартиране, без да се зарежда Windows, така че всеки постоянен злонамерен софтуер да изпита трудности, за да се скрие или защити. Изпълнете го, когато се притеснявате, че устройството е бил изложено на злонамерен софтуер или вирус или ако искате да сканирате вашето устройство, без да се свързвате с интернет. Това ще рестартира устройството, така че не забравяйте да запишете файловете, които може да сте отворили.



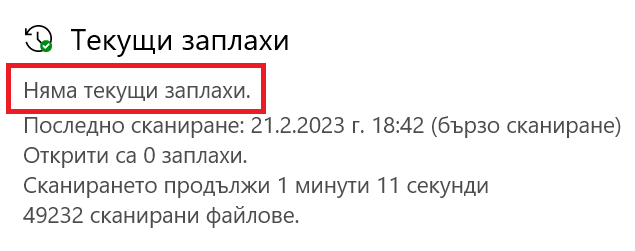
Фигура 5. Windows Security, Защита от вируси и заплахи - Опции за сканиране



Фигура 6. Защита от вируси и заплахи - Опция Пълно сканиране



Фигура 7. Защита от вируси и заплахи – изпълнение на пълно сканиране



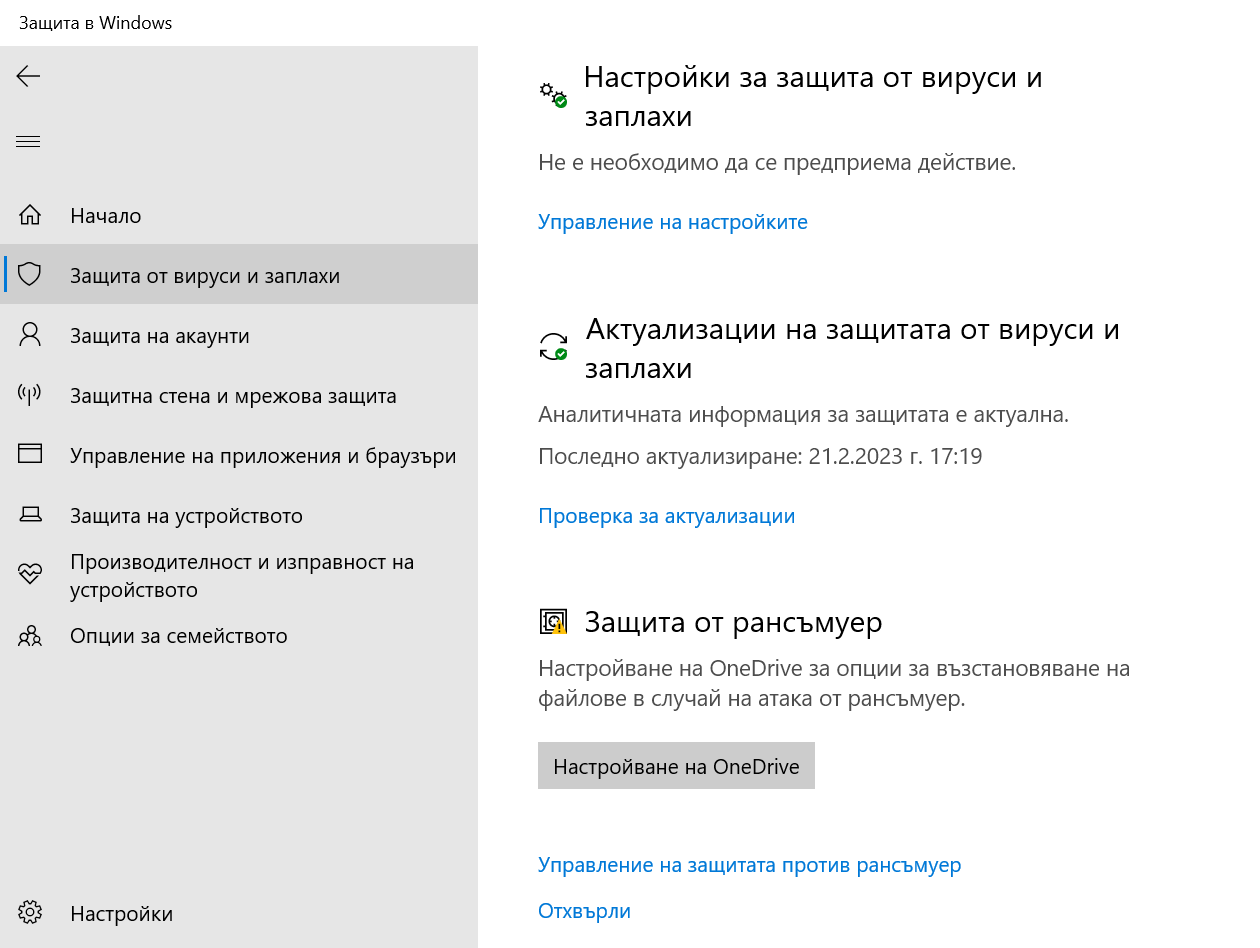
Фигура 8. Статус за текуща защита

Съществуват много други настройки, като например, ако искате да персонализирате Вашето ниво на защита, можете да използвайте **Управление на настройките**/**Настройките на защитата от вируси и заплахи**. *Например, когато искате да, да изпращате примерни файлове на Microsoft, да изключвате доверени файлове и папки от многократно сканиране или, за да изключите защитата си временно.*

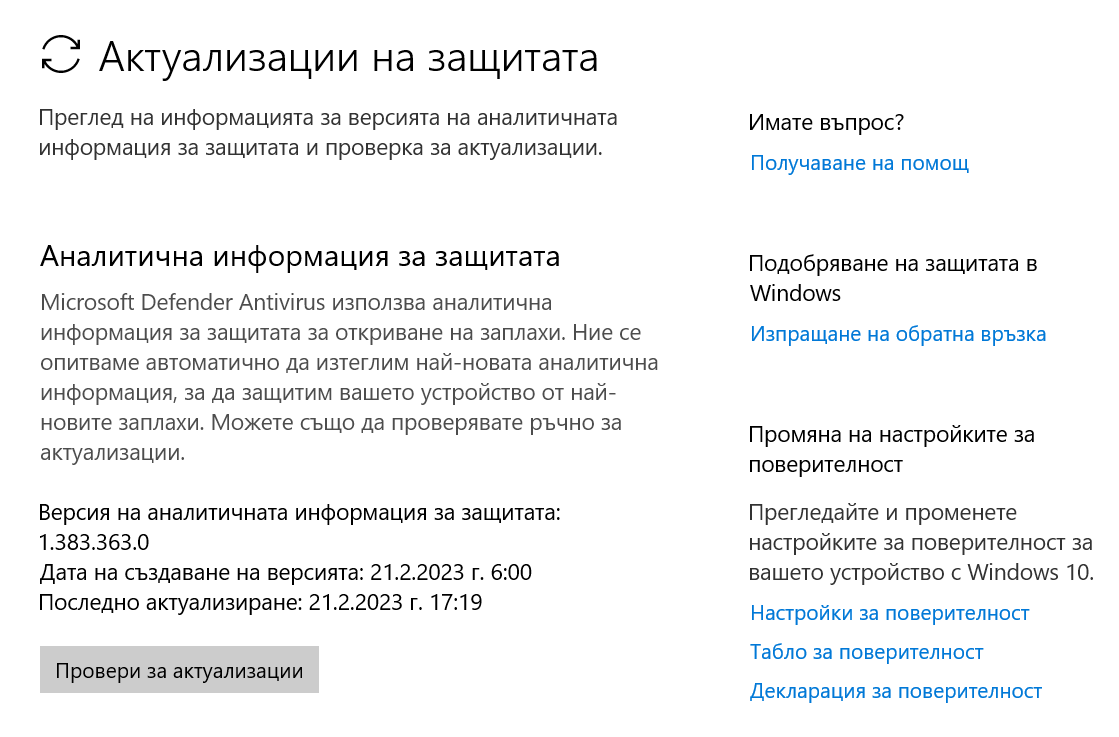
## Защита на устройството с най-новите актуализации

Аналитичната информация за защитата (понякога наричана "дефиниции") са файлове, които съдържат информация за най-новите заплахи, които могат да заразят вашето устройство. "Windows Security" използва аналитична информация за защита всеки път, когато се изпълнява сканиране.

Майкрософт (Microsoft) автоматично изтегля най-новата аналитична информация на вашето устройство като част от обновяването на Windows (Windows Update), но можете също така ръчно да проверите за нея. На страницата "З**ащита от вируси и заплахи**", под **Актуализации на защитата от вируси и заплахи (Virus and Threat Protection Settings)**, изберете **Проверка за актуализации** за сканиране за най-новата аналитична информация за защитата (**Check for Updates**). (Фигура 9), (Фигура 10).



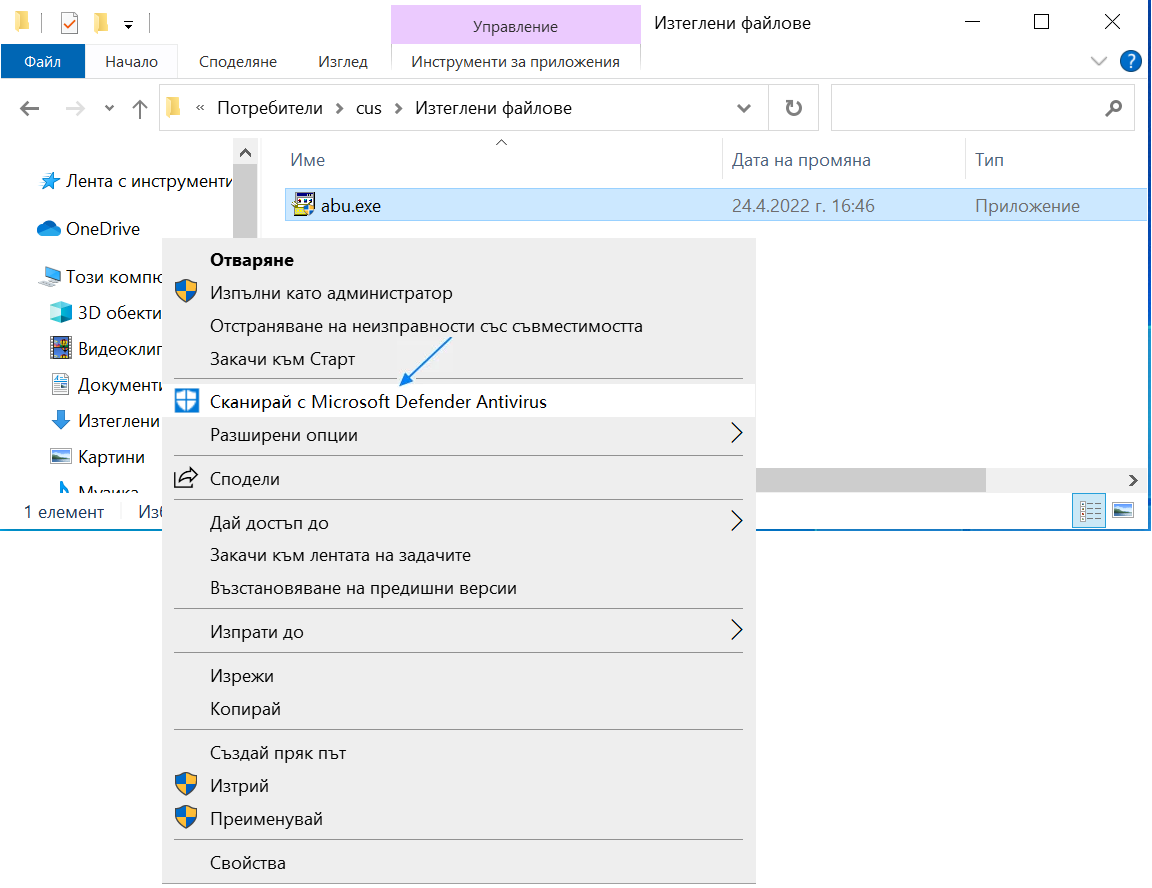
Фигура 9. Защита от вируси и заплахи - Обновявания



Фигура 10. Обновявания на дефинициите за заплахи

## Ръчно изпълнение на сканиране за злонамерен софтуер

Ако се притеснявате за конкретен файл или папка на локалното си устройство, можете да щракнете с десния бутон върху файла или папката във Файлов мениджър (File Explorer), след което да изберете сканиране с Microsoft Defender антивирус. (Фигура 11)



Фигура 11. Ръчно сканиране на файл с Windows Defender

Ако подозирате, че има злонамерен софтуер или вирус на вашето устройство, трябва незабавно да изпълните бързо сканиране.

## Включване или изключване на защитата Microsoft Defender Antivirus

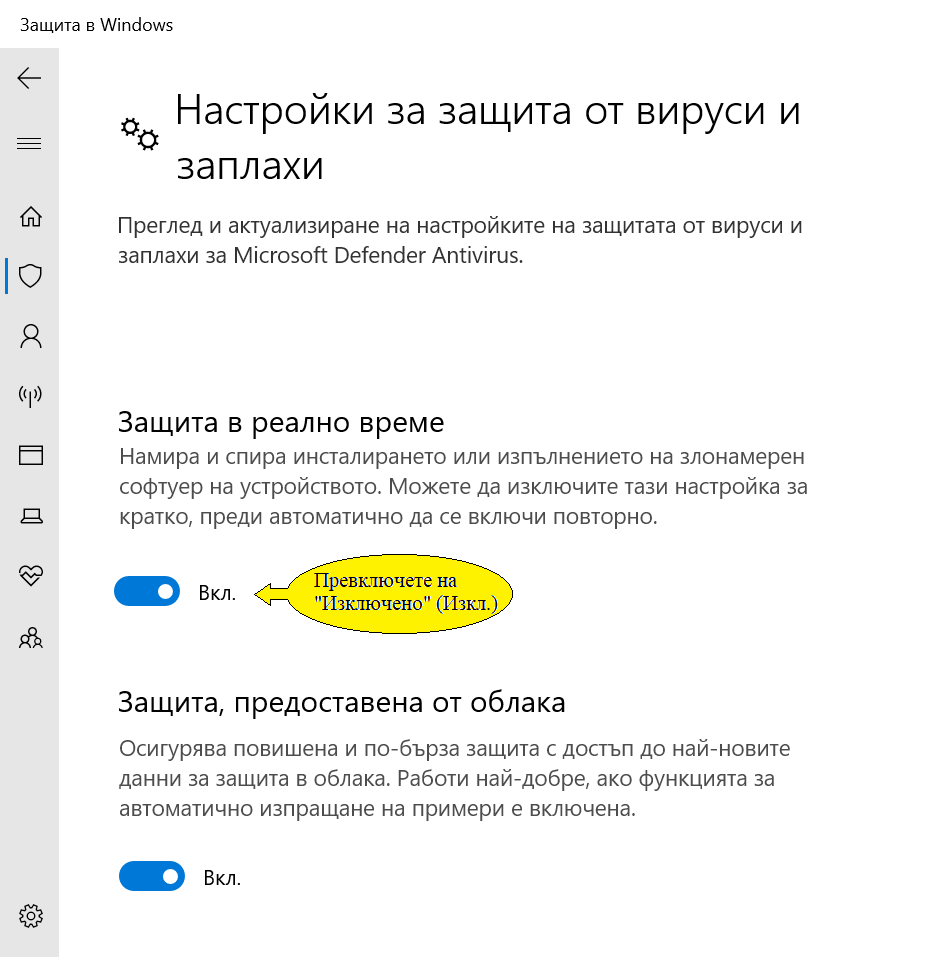
Понякога може да се наложи да спрете за кратко изпълнението на защитата в реално време на Windows Defender. Докато защитата в реално време е изключена, файловете, които отваряте или изтегляте, няма да се сканират за заплахи. Въпреки това защитата в реално време автоматично ще се включи отново скоро, за да осигури защита на вашето устройство.

**Временно изключване на защитата в реално време**

Изберете Старт > Настройки > Актуализиране и защита > Защита в Windows и след това Защита от вируси и заплахи > Управление на настройките. (В ранните версии на Windows 10 изберете Защита от вируси и заплахи > Настройки за защита от вируси и заплахи.)

Променете настройката **Защита в реално време** на **Изключено** и изберете Да, за да потвърдите. (Фигура 12)

Windows Defender не може да бъде деинсталиран, но може да бъде спрян/изключен.



Фигура 12. Изключване на защитата в реално време на Windows Defender

## Деинсталиране на антивирусен софтуер

Ако имате администраторски права, можете да деинсталирате (uninstall) допълнително инсталиран антивирусен софтуер.

Това става по същия начин както, ако искате да деинсталирате или поправите (modify) някое приложение в Windows, ако то не се изпълнява правилно.

За да го направите, изберете бутон Старт -> Настройки -> Приложения -> Приложения и функции (Start -> Settings -> Apps -> Apps & features) и изберете приложението, което искате да поправите/деинсталирате.

## Използвана литература

* Останете защитени със "Защита в Windows" - <https://support.microsoft.com/bg-bg/windows/останете-защитени-със-защита-в-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963>
* [Fix] Windows Defender Yellow Exclamation Icon and “Set up OneDrive” Warning - https://www.winhelponline.com/blog/set-up-onedrive-yellow-exclamation-defender-security-center/
* Windows 10’s Defender fails with threat service has stopped error - <https://www.windowslatest.com/2020/04/16/windows-defender-bug-causes-threat-service-has-stopped/>
* How to Scan with Microsoft Defender Antivirus on Windows 10 - <https://www.howtogeek.com/679263/how-to-scan-with-microsoft-defender-antivirus-on-windows-10/>
* Perform a virus scan – Windows 10 and 11 - <https://www.rrc.ca/its/help-resources/security/perform-a-virus-scan-windows-10/>
* How To Manually Check For Virus and Threat Protection Updates On Windows 10? -https://mywindowshub.com/how-to-manually-check-for-virus-and-threat-protection-updates-on-windows-10/
* How to Use Windows Defender to Scan a Folder for Malware - <https://www.bleepingcomputer.com/tutorials/how-to-use-windows-defender-to-scan-a-folder-for-malware/>
* How to Enable or Disable Real-time Protection for Microsoft Defender Antivirus in Windows 10 - <https://www.tenforums.com/tutorials/3569-turn-off-real-time-protection-microsoft-defender-antivirus.html>