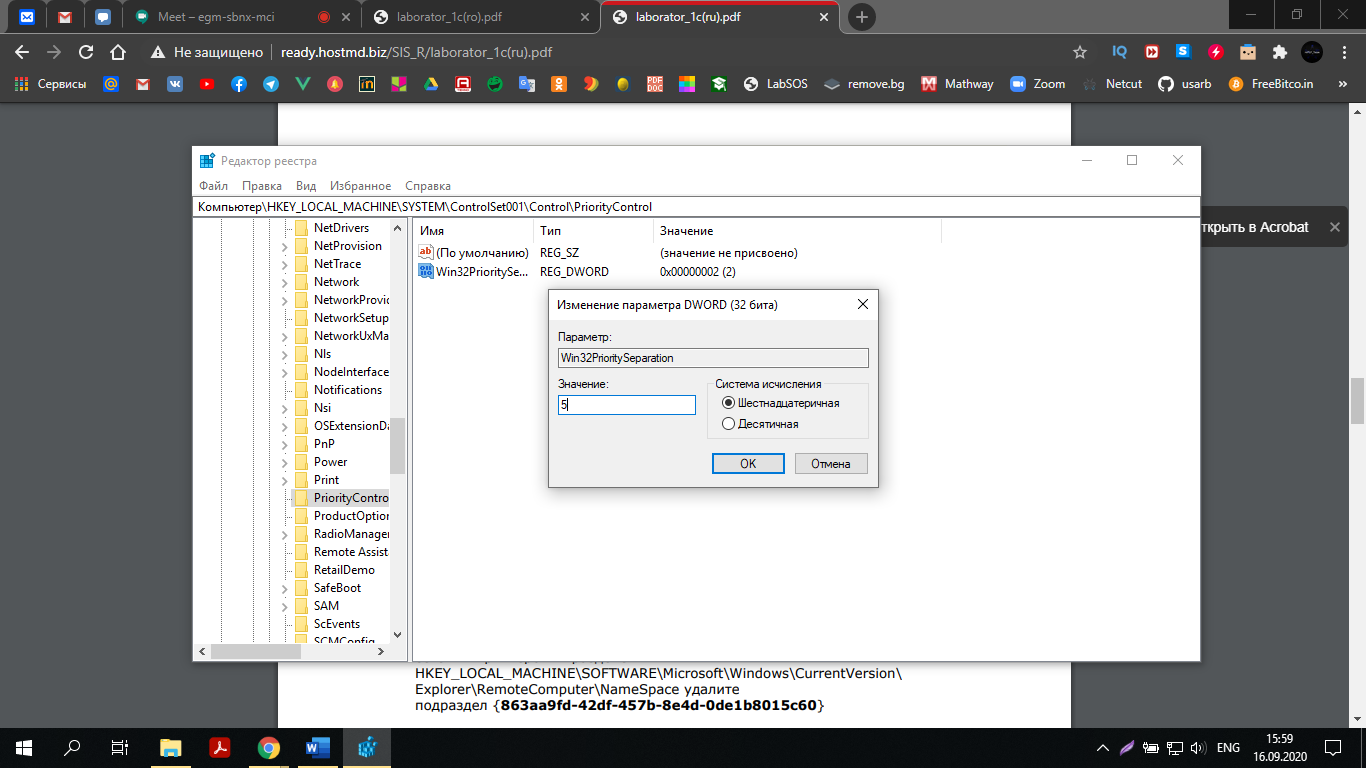
**Laborator nr. 3 Sisteme de operare si securitatea calculatorului**

Elaborat: Bazaochi Dumitru

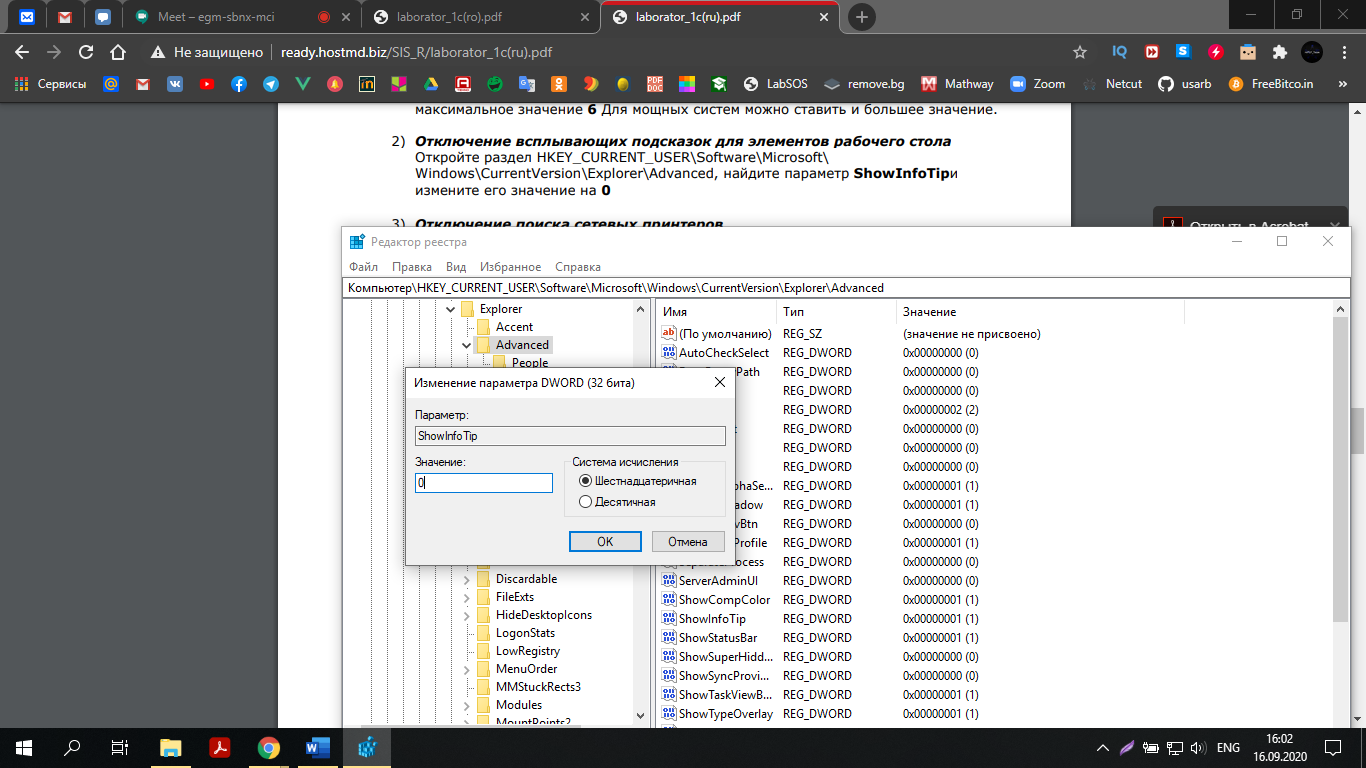
1. **Creșterea priorității cererii în prezent active**

Aplicatia Windows rulează într-un mod activ și în fundal. Dacă doriți ca aplicația activă să devină în mai multe resurse și, prin urmare ruleze mai repede, în secțiunea HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\PriorityControl localizați Win32PrioritySeparation. Valoarea implicită este 2. Valoarea maximă a 26, dar dacă aveți un sistem nu este suficient de puternic, este necesar de a schimba această setare cu precauție. Recomandat pentru aceste sisteme valoarea maximă a 6 pentru sistemele puternice pot fi setate și mai mult.



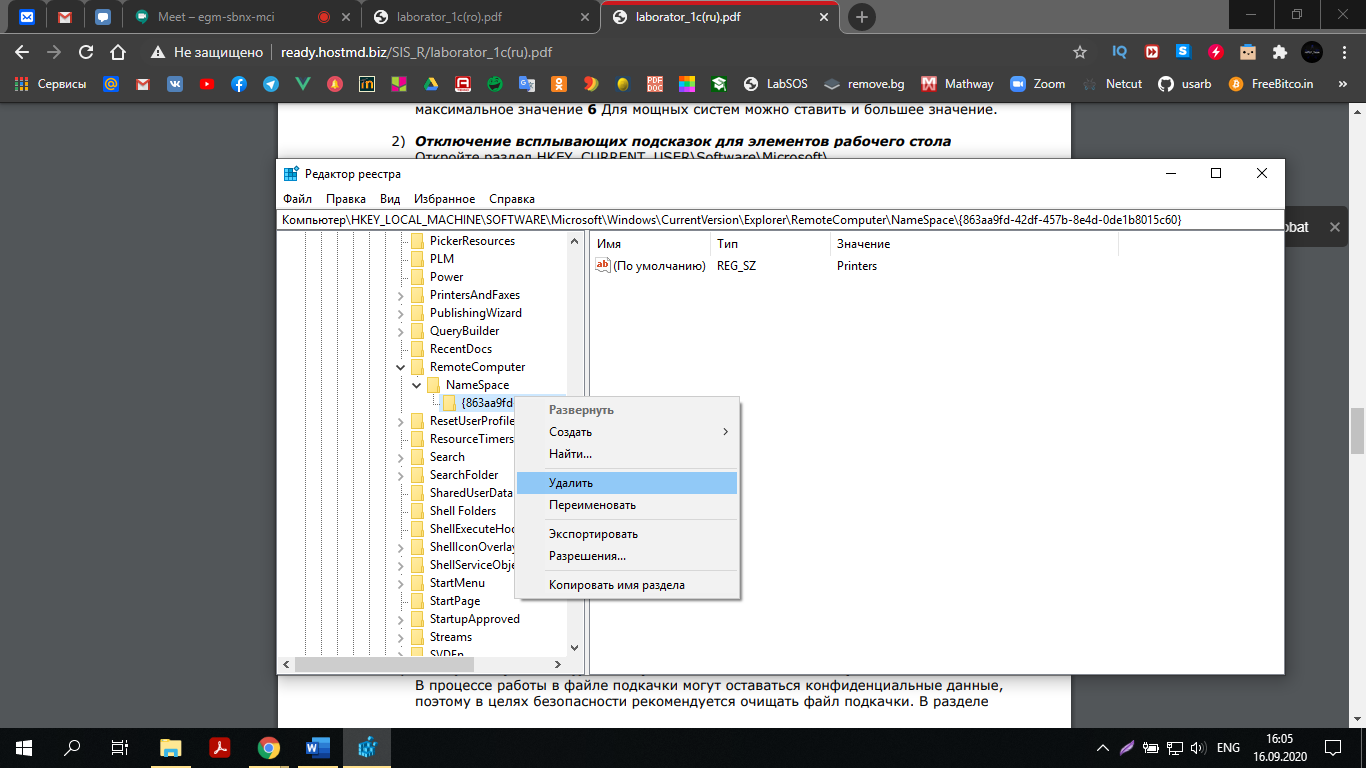
1. **Deconectarea auxiliarelor(hits) desctop**

Localizați HKEY\_CURRENT\_USER\Software\Microsoft\ Windows\CurrentVersion\Explorer\Advanced, găsiți ShowInfoTipи modificați în 0



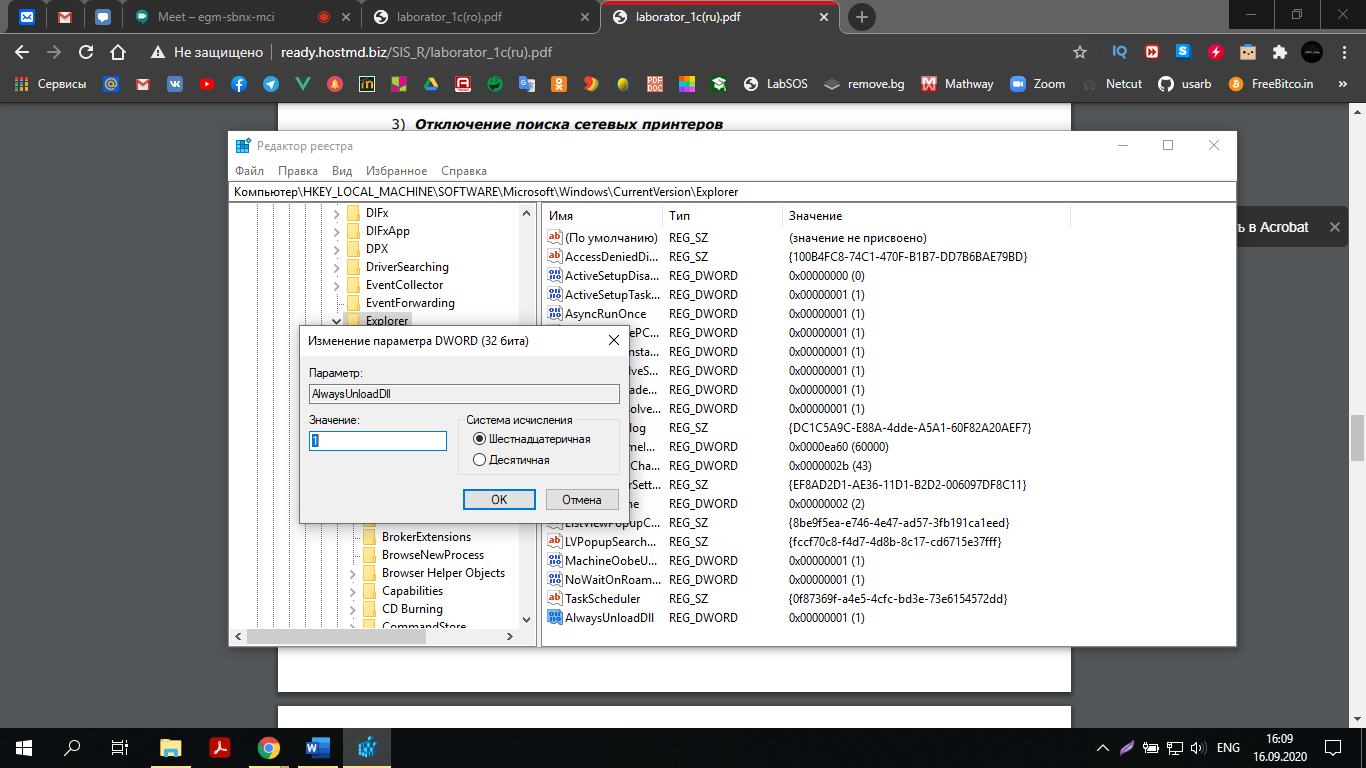
1. Opriți căutarea imprimantelor de rețea

Dacă nu există nici LAN -imprimante de rețea, puteți dezactiva căutarea pentru imprimantele de rețea. Secțiune HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\RemoteComputer\NameSpace omiteți {863aa9fd-42df-457b-8e4d0de1b8015c60}



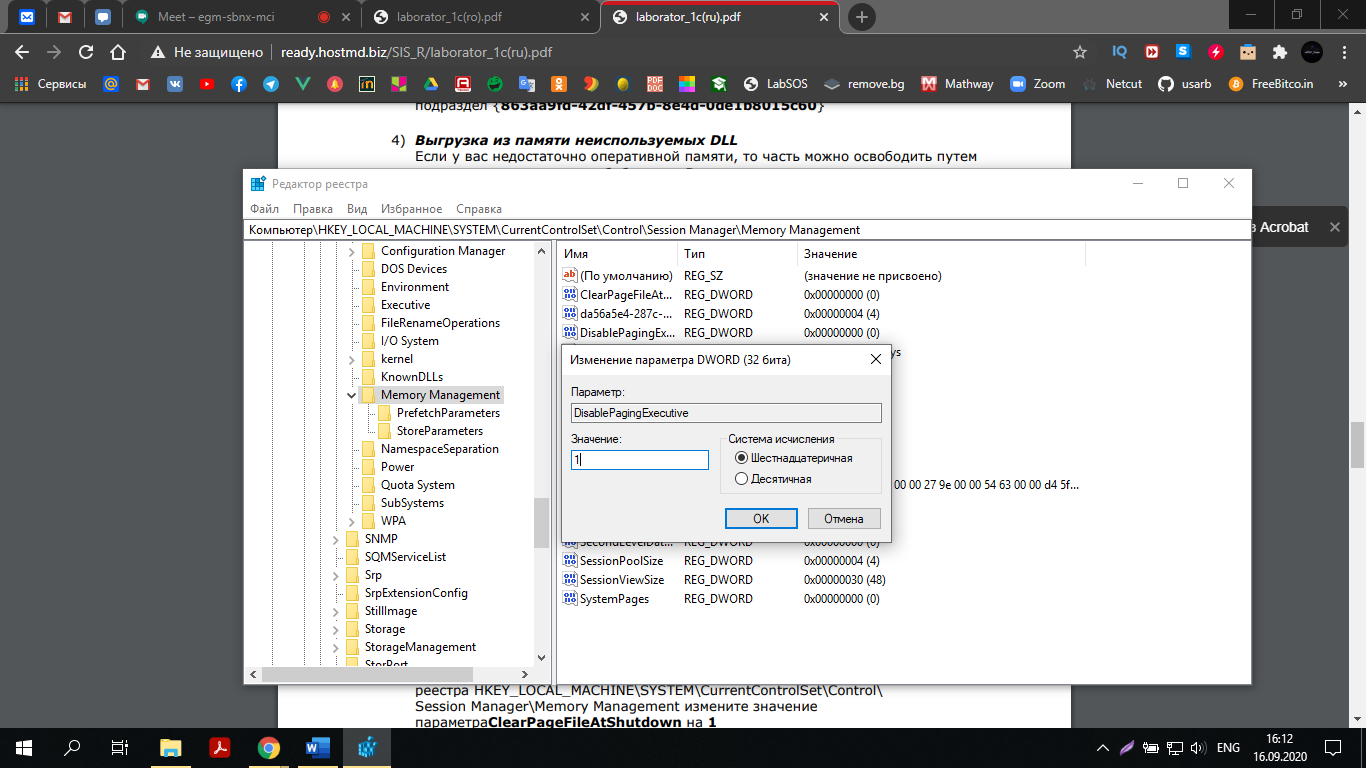
1. Descărcarea din gestiunea memoriei a DLL neutilizate

Dacă nu aveți destul RAM, o parte poate fi eliberat prin descărcare biblioteci neutilizate. În secțiunea de deschidere a registrului HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Explorer creem paramerul de tip DWORD сu numele AlwaysUnloadDll. și valoarea 1



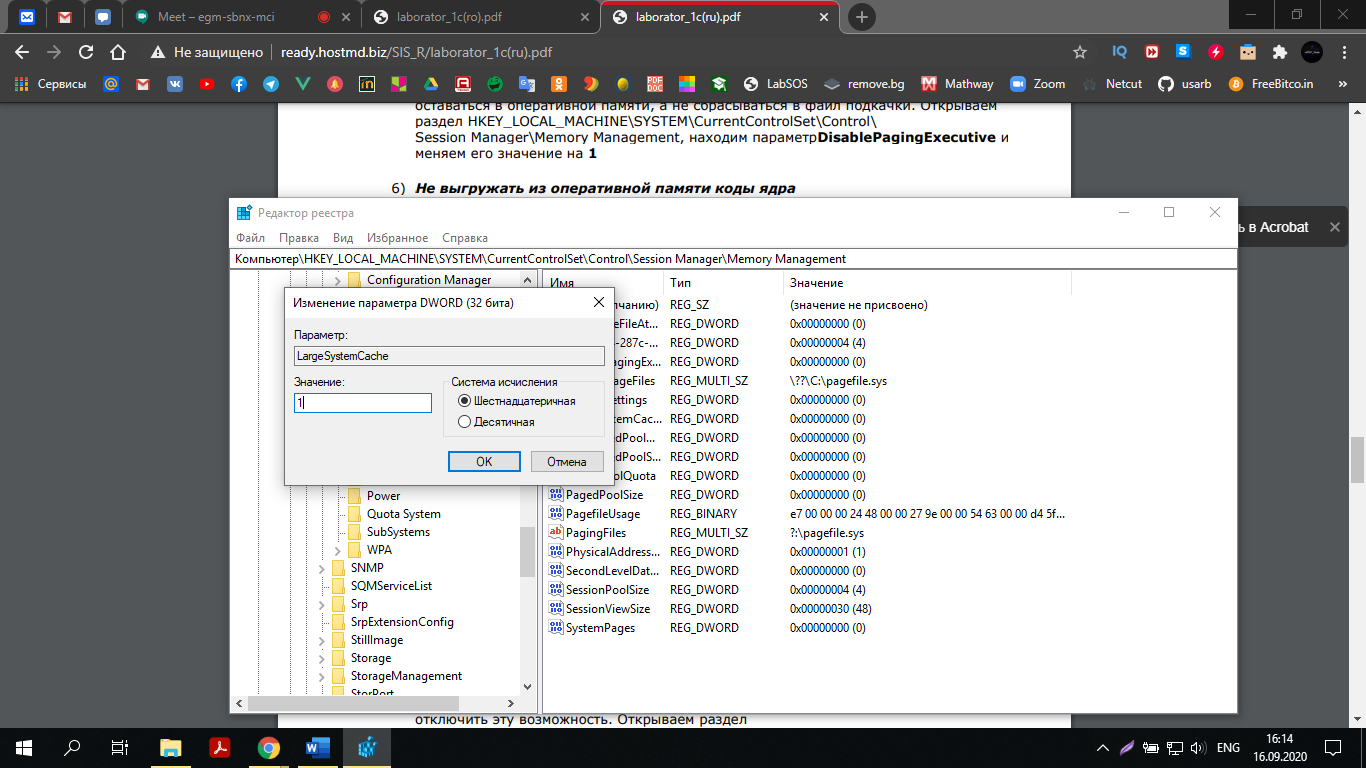
1. De a nu descărca din memoria operativă a nucleelor de coduri și driverelor

În cazul în care computerul are 2 GB sau mai mult de RAM, cererile vor fi mai rapid prelucrare de utilizator în cazul în care kernel-ul și driver-ul va rămâne în memorie, și să nu arunce în fișierul de paginare. Deschidem secțiunea HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management, găsim parametrul DisablePagingExecutive și-l modificăm pe 1



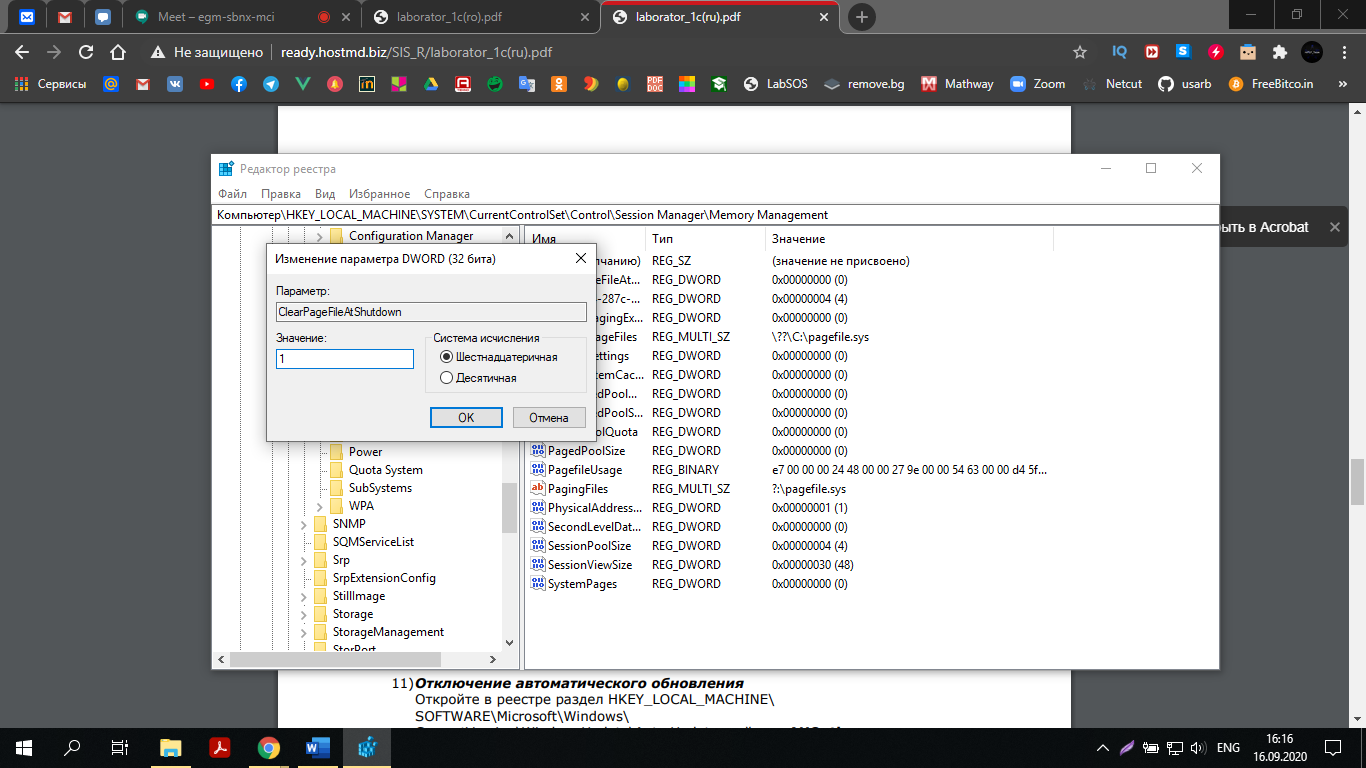
1. De a nu descărca din memorie kernel-lurile

Modificarea acestei setări nu va descărca kernel, și va lucra direct în memorie, și nu încărcați diferite module de pe hard disk. deschis Secțiunea HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management modificăm LargeSystemCache pe 1



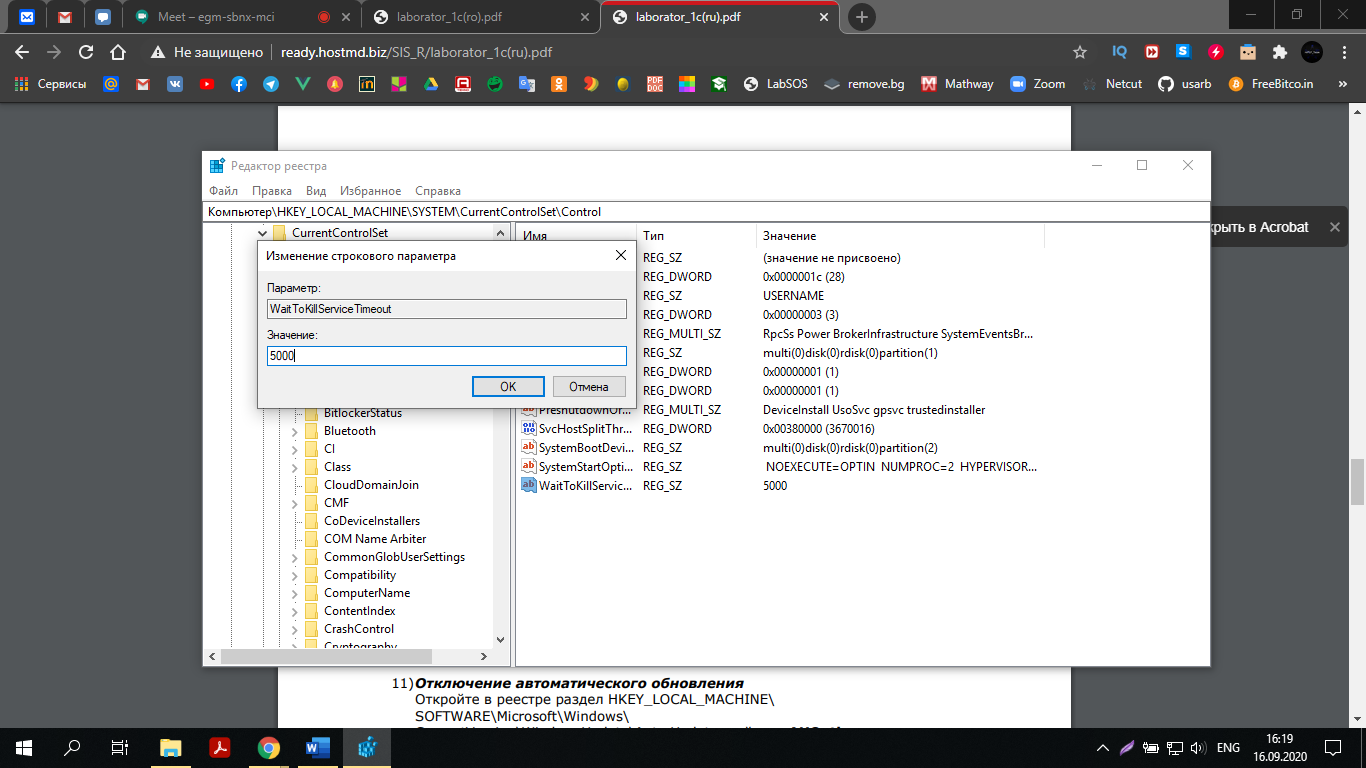
1. Curățarea fișierul de paginare de la închidere

În timpul funcționării în fișierul de paginare poate rămâne date confidențiale, astfel din motive de siguranță, se recomandă pentru a șterge fișierul de swap. În secțiunea HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management modificați parametrul ClearPageFileAtShutdown pe 1



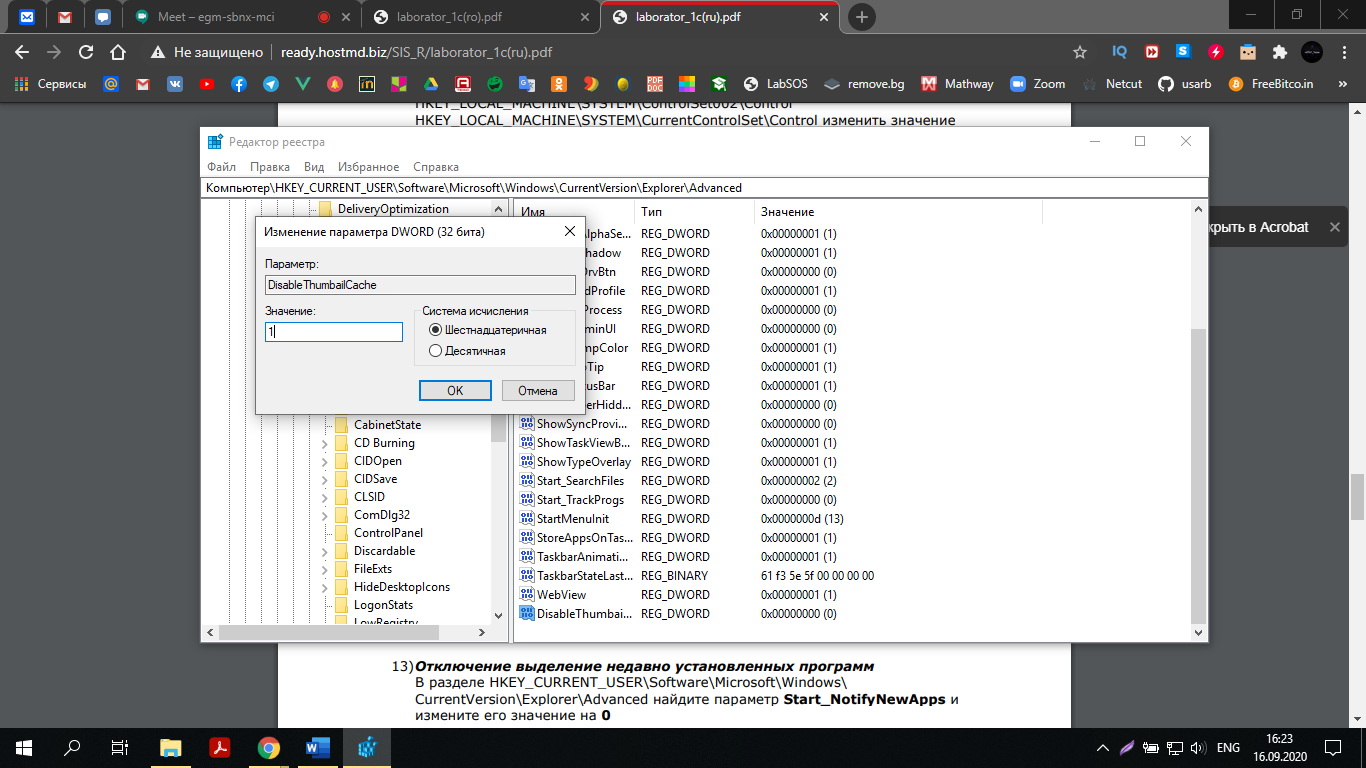
1. Deconectarea rapidă a sistemului de calcul

Dacă sistemul nu este oprit pentru o lungă perioadă de timp, încercați secțiunile HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet002\Control HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control modifica valoarea WaitToKillServiceTimeout de 20000 (implicit) pe, de exemplu 12000 (12 s.)

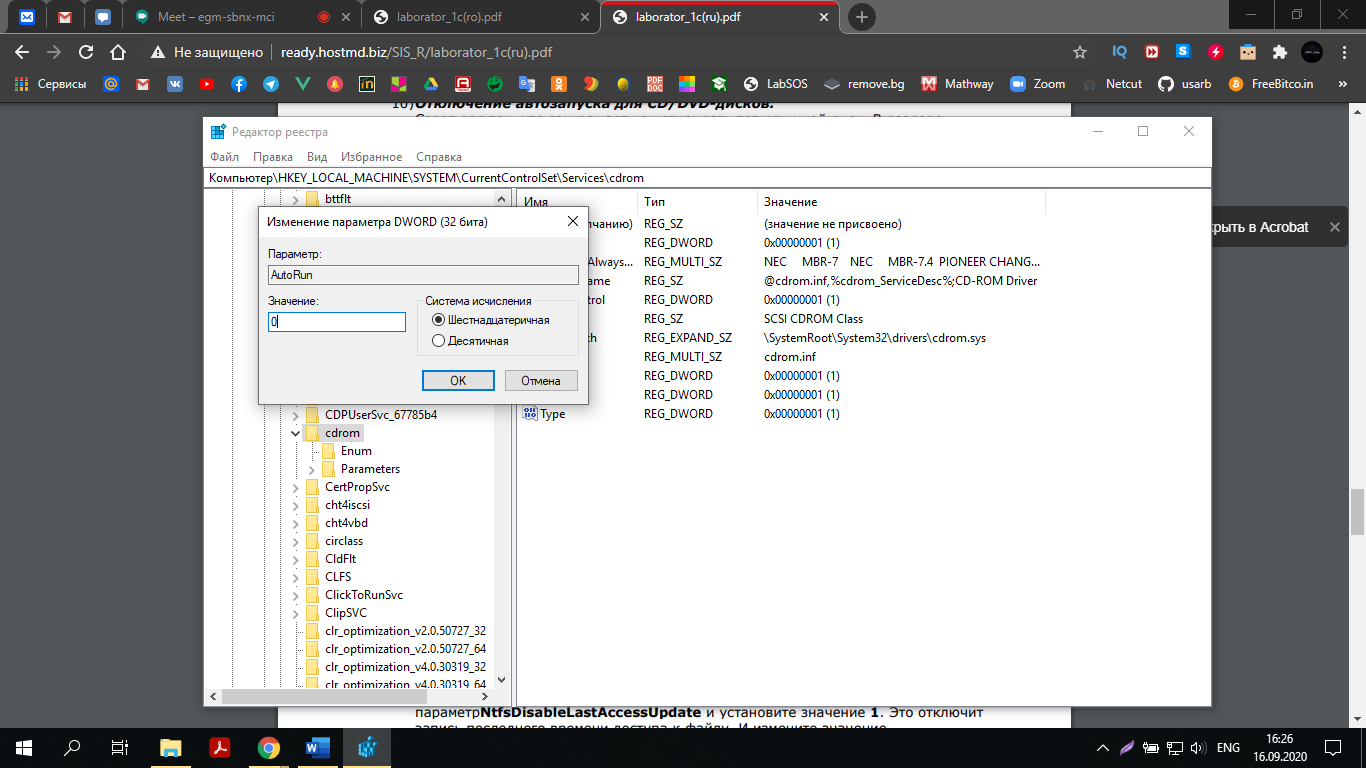


1. Desconectarea cashing al imaginilor.

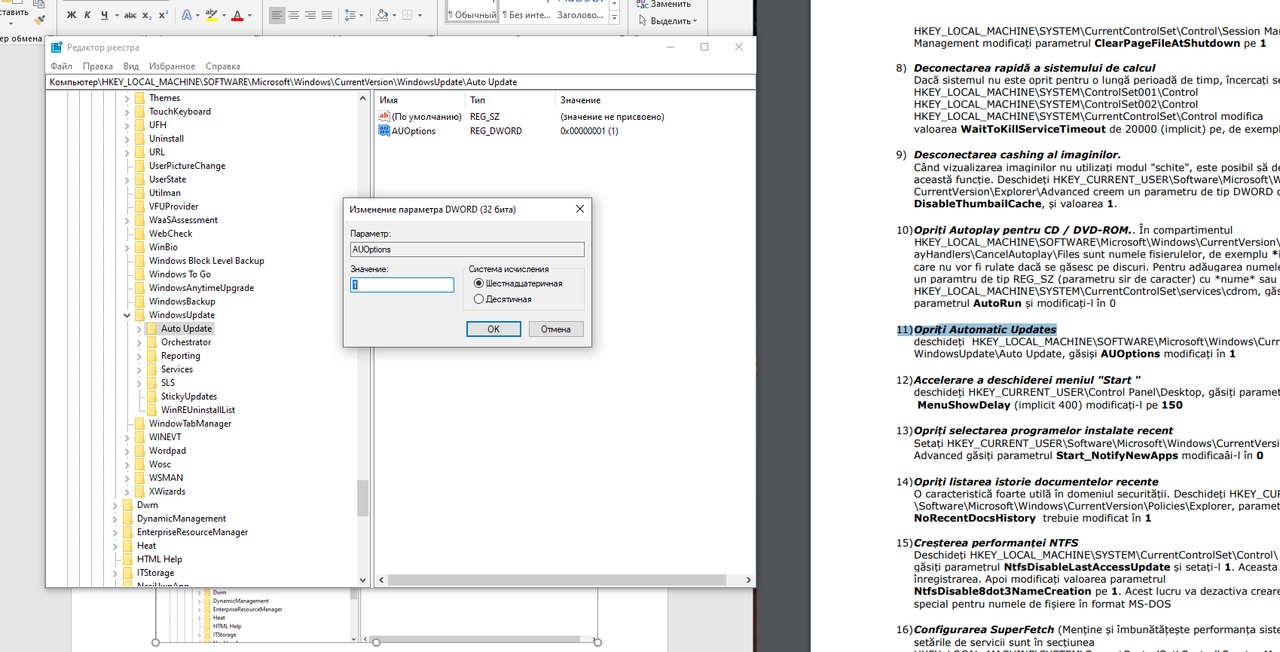
Când vizualizarea imaginilor nu utilizați modul "schite", este posibil să dezactivați această funcție. Deschideți HKEY\_CURRENT\_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\Advanced creem un parametru de tip DWORD cu numele DisableThumbailCache, și valoarea 1.



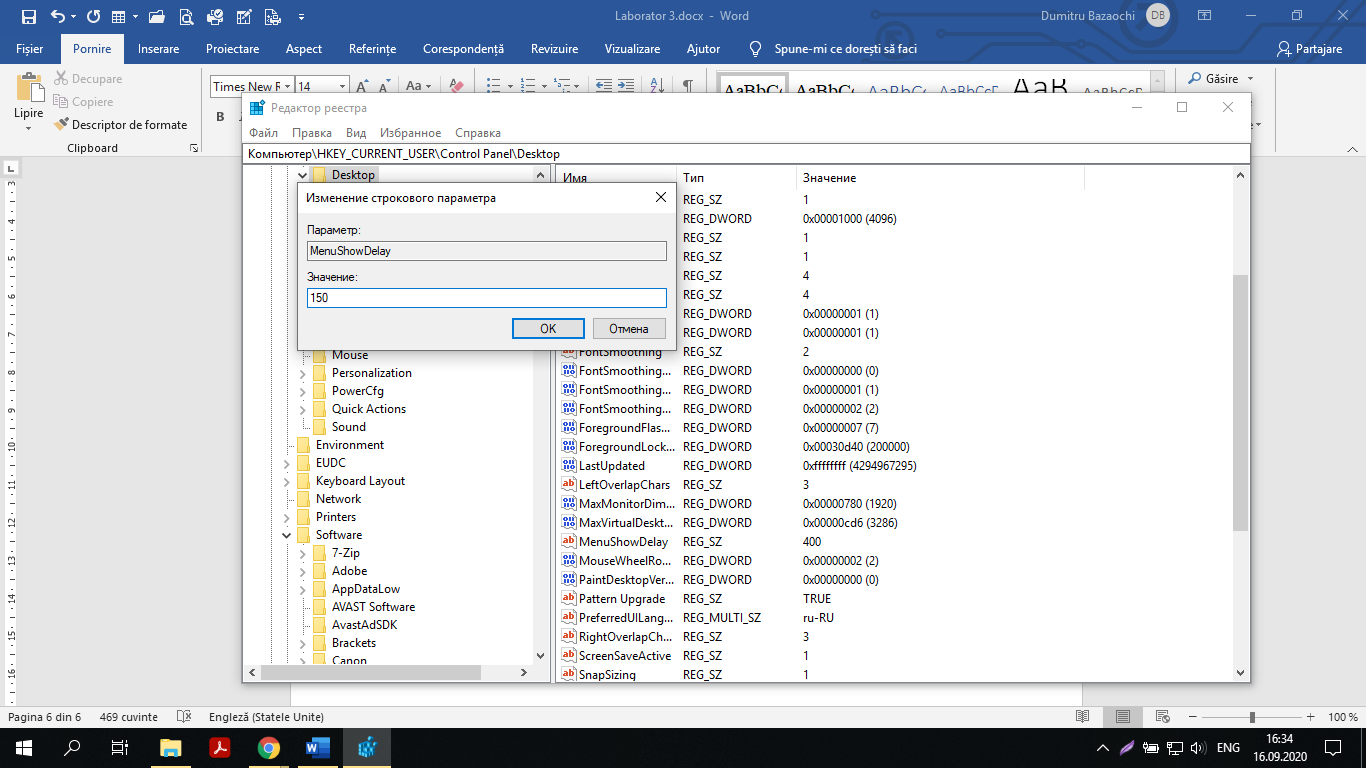
10)Opriți Autoplay pentru CD / DVD-ROM.. În compartimentul HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Autopl ayHandlers\CancelAutoplay\Files sunt numele fisierulelor, de exemplu \*instal\*.bat, care nu vor fi rulate dacă se găsesc pe discuri. Pentru adăugarea numele trebuie creat un paramtru de tip REG\_SZ (parametru sir de caracter) cu \*nume\* sau deschideți HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\cdrom, găsiți parametrul AutoRun și modificați-l în 0



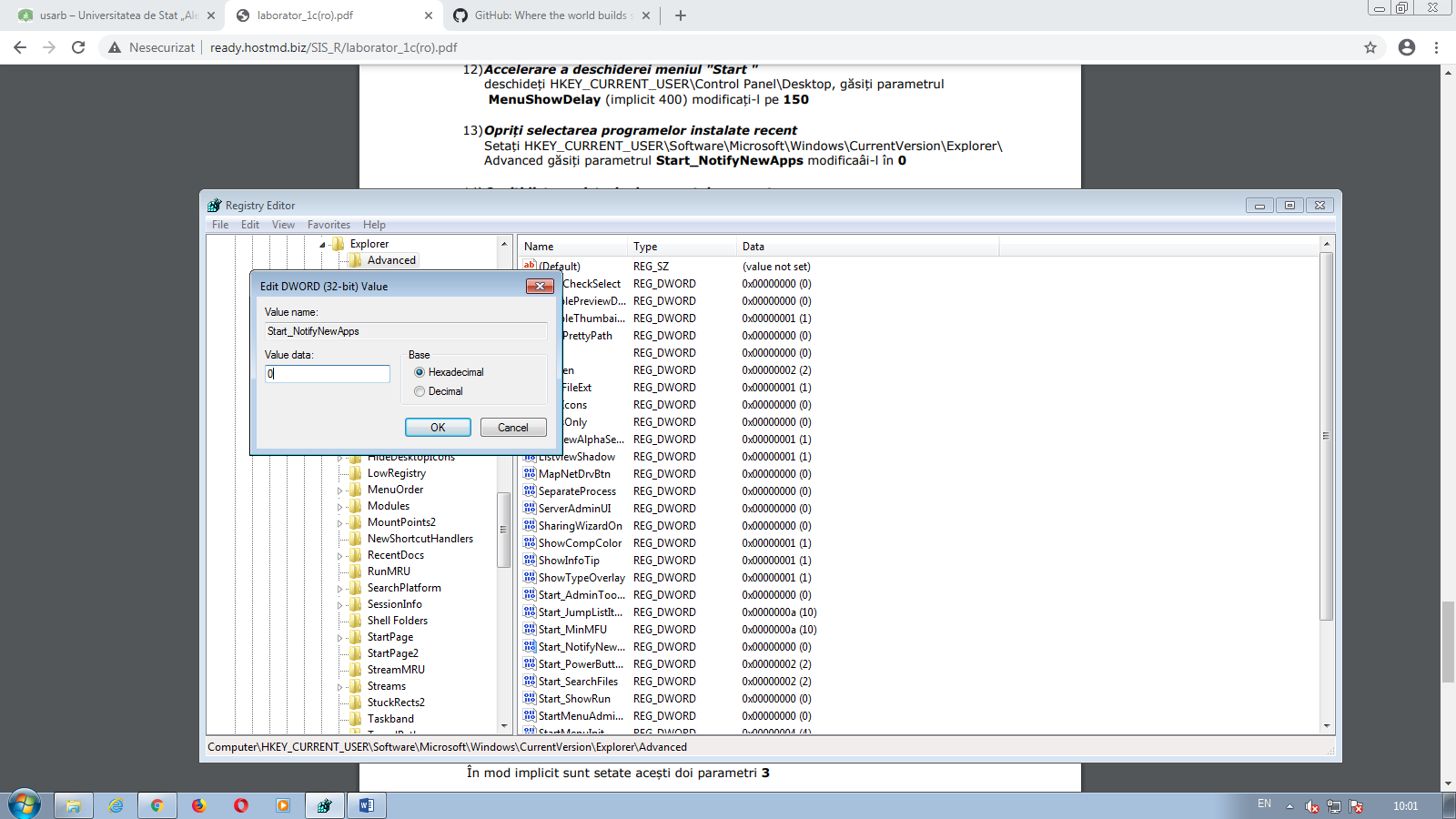
11)Opriți Automatic Updates deschideți HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ WindowsUpdate\Auto Update, găsiși AUOptions modificați în 1



12) Accelerare a deschiderei meniul "Start " deschideți HKEY\_CURRENT\_USER\Control Panel\Desktop, găsiți parametrul MenuShowDelay (implicit 400) modificați-l pe 150

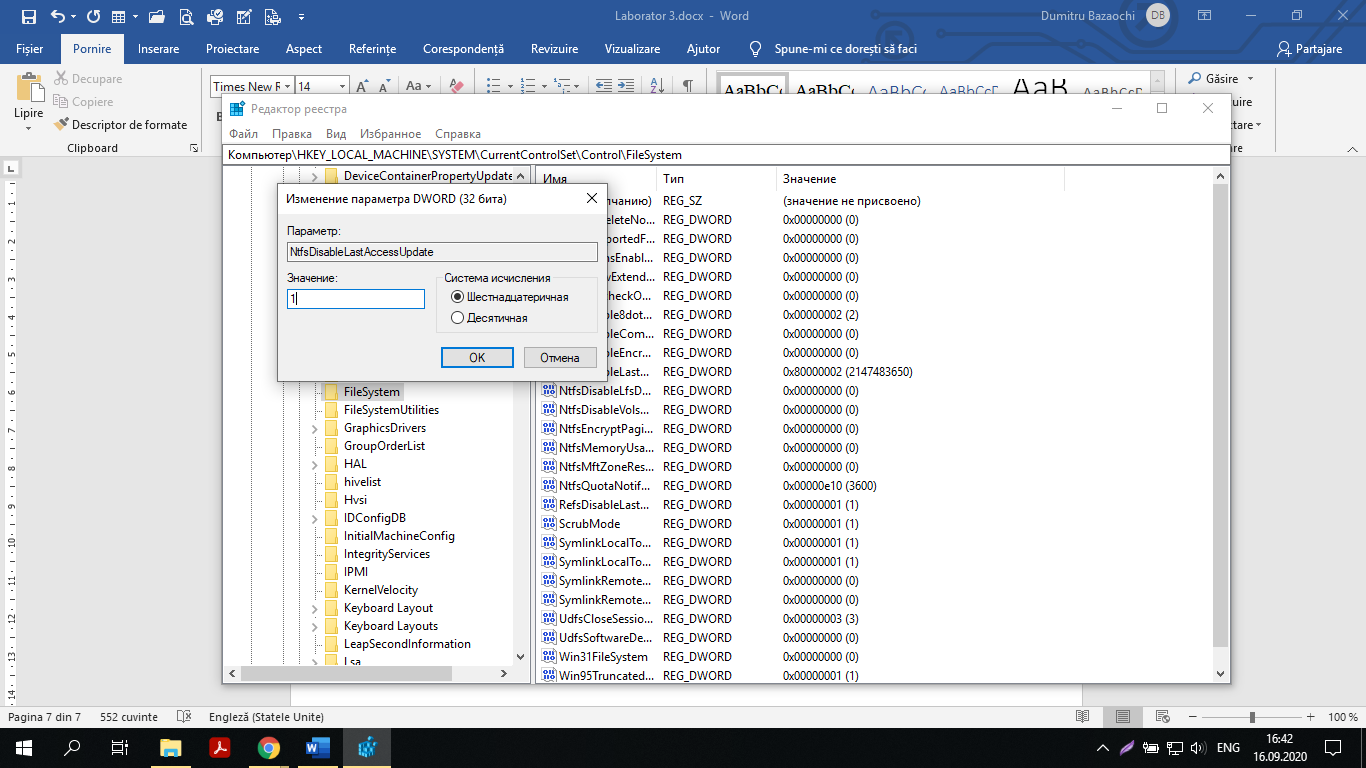


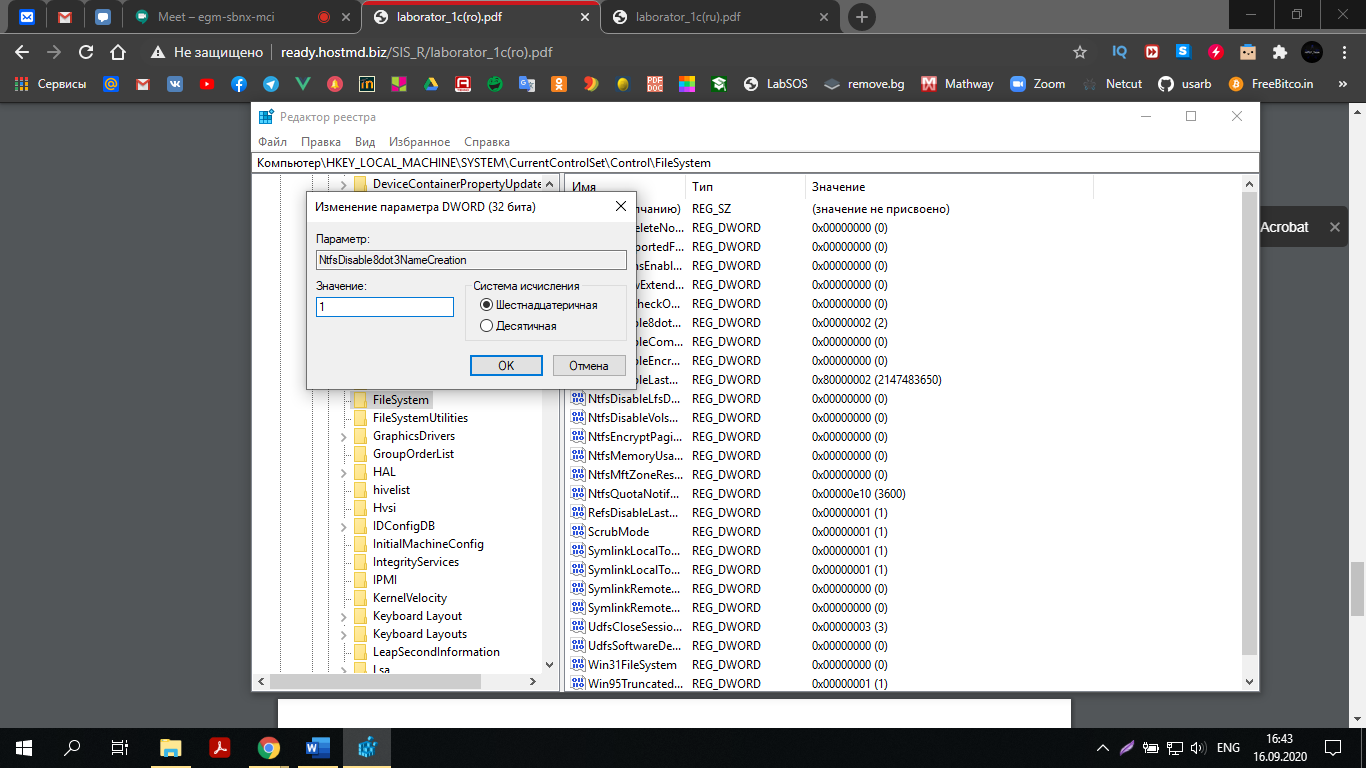
13) Opriți selectarea programelor instalate recent Setați HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ Advanced găsiți parametrul Start\_NotifyNewApps modificaâi-l în 0

14)Opriți listarea istorie documentelor recente O caracteristică foarte utilă în domeniul securității. Deschideți HKEY\_CURRENT\_USE \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, parametrul NoRecentDocsHistory trebuie modificat în 1

--- nu am gasit, lipseste

15) Creșterea performanței NTFS Deschideți HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ FileSystem, găsiți parametrul NtfsDisableLastAccessUpdate și setați-l 1. Aceasta va deconecta înregistrarea. Apoi modificați valoarea parametrul NtfsDisable8dot3NameCreation pe 1. Acest lucru va dezactiva crearea unui tabel special pentru numele de fișiere în format MS-DOS





16) Configurarea SuperFetch (Menține și îmbunătățește performanța sistemului.) Toate setările de servicii sunt în secțiunea HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters există trei parametri care definesc funcționarea și serviciul.

EnableBootTrace - dezactivează serviciul de urmărire. Includ urmărirea este necesară numai în cazul în care serviciul nu funcționează corespunzător.

EnablePrefetcher - deconectăm mecanismul Prefetcher (prefetching)

EnableSuperfetch - acesta include servicii Superfetch. Astfel încît parametri EnablePrefetcher и EnableSuperfetch au următoarele valori:

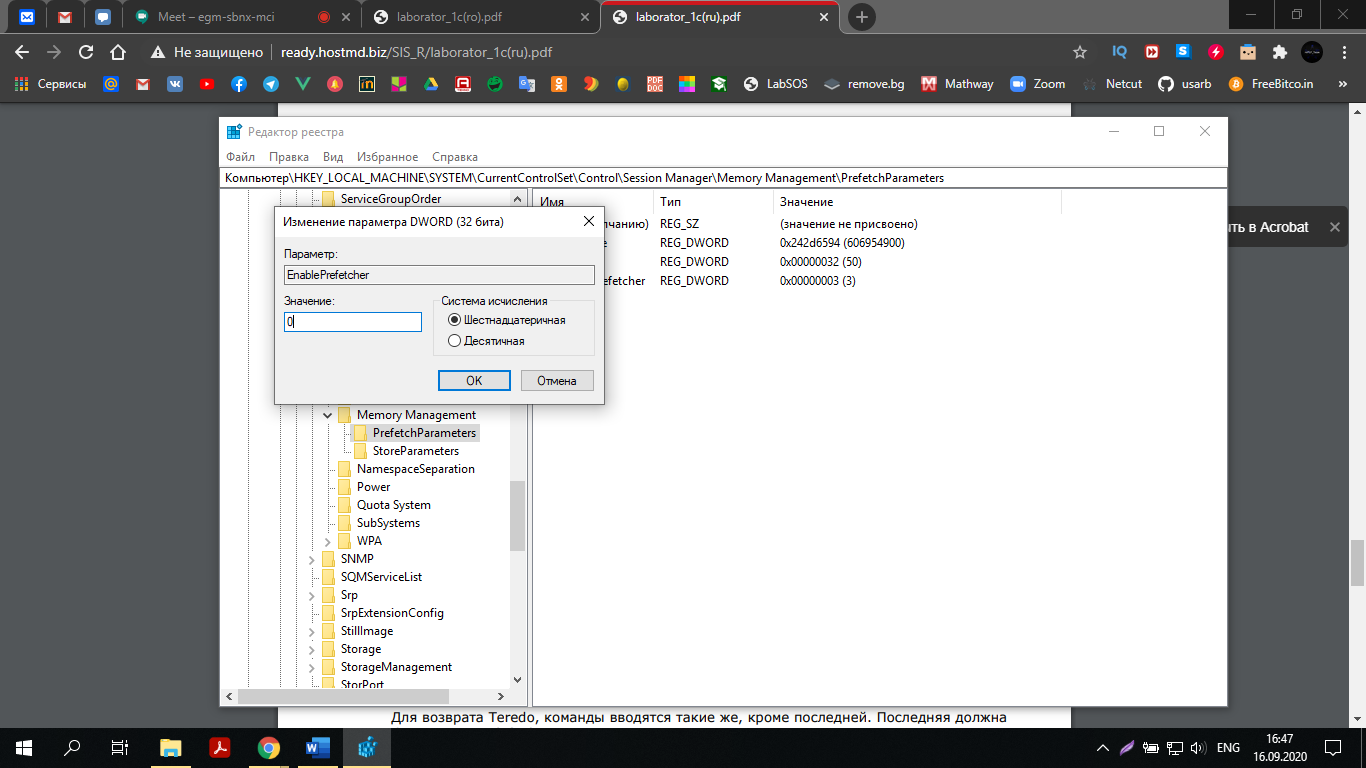
• 0 - funcție este activată

• 1 - caracteristică este activată numai pentru pornire

• 2 - Funcția este activată în timpul funcționării, dar este dezactivat la pornirea sistemului

• 3 - funcție este activată în toate modurile

În mod implicit sunt setate acești doi parametri 3



17) Dezactivați protocol Teredo

Protocol Teredo în Windows 7 este potențial vulnerabile la atac - spun expertii Symantec. Dezactivați proxy Teredo poate accelera de rețea și Internet. Începeți un prompt de comandă (Run) și introduceți comanda la un moment dat.

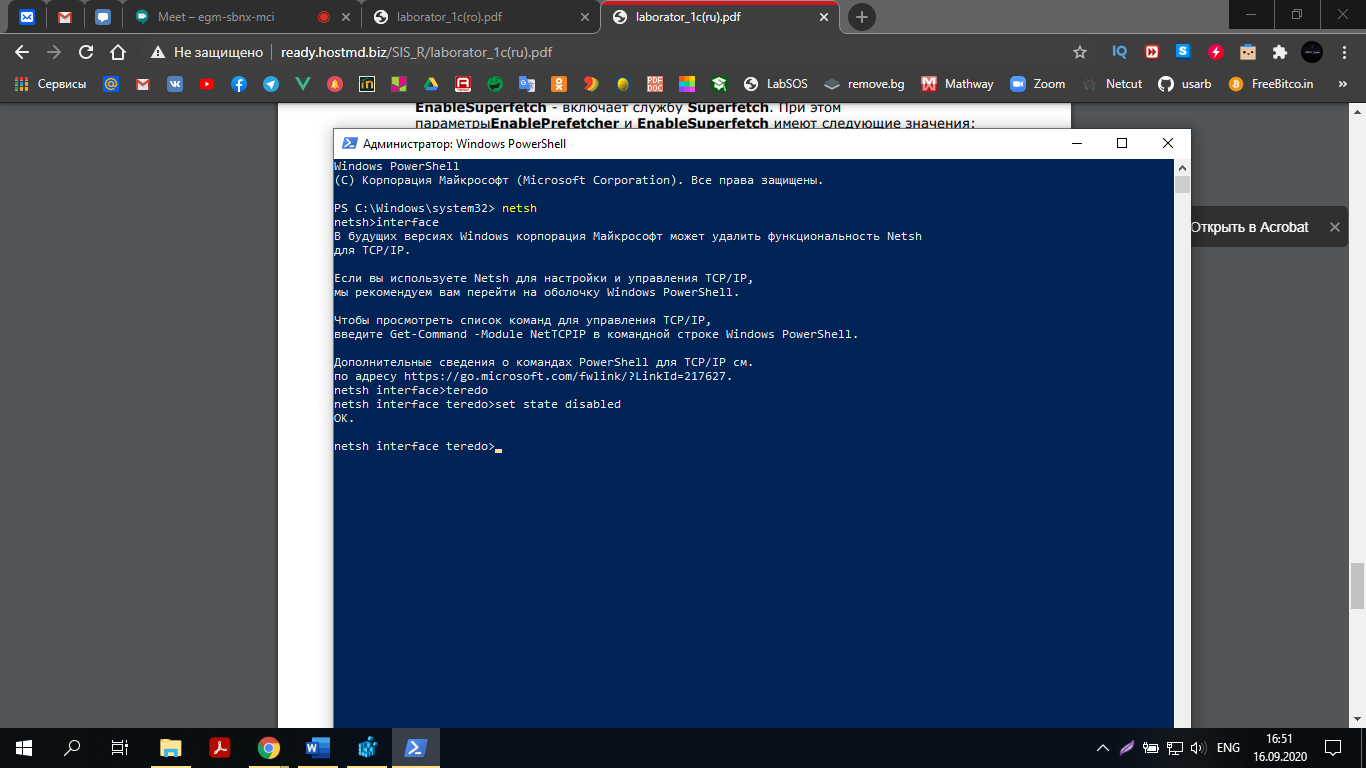
netsh

interface

teredo

set state disabled

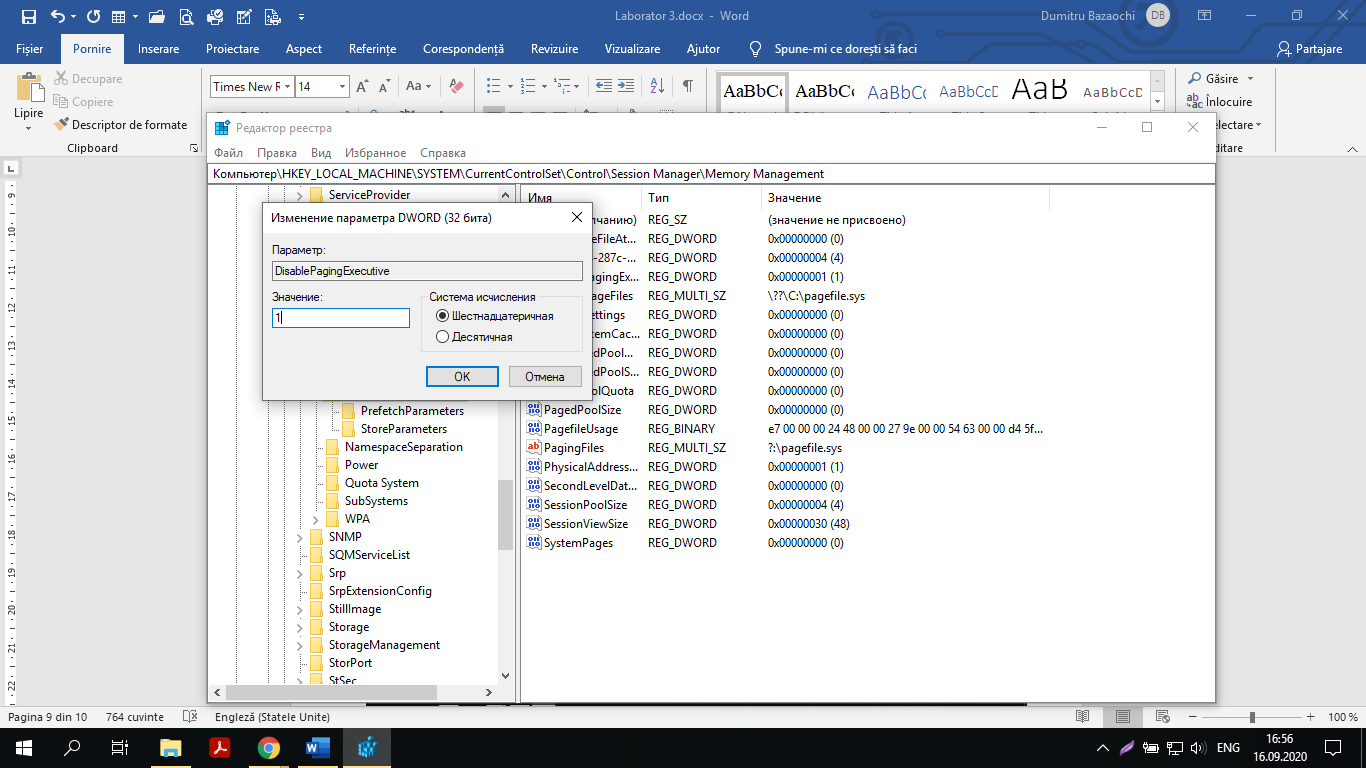
Pentru a reveni Teredo, comenzile sunt la fel, cu excepția ultimului. Aceasta din urmă ar trebui să fie statset state default

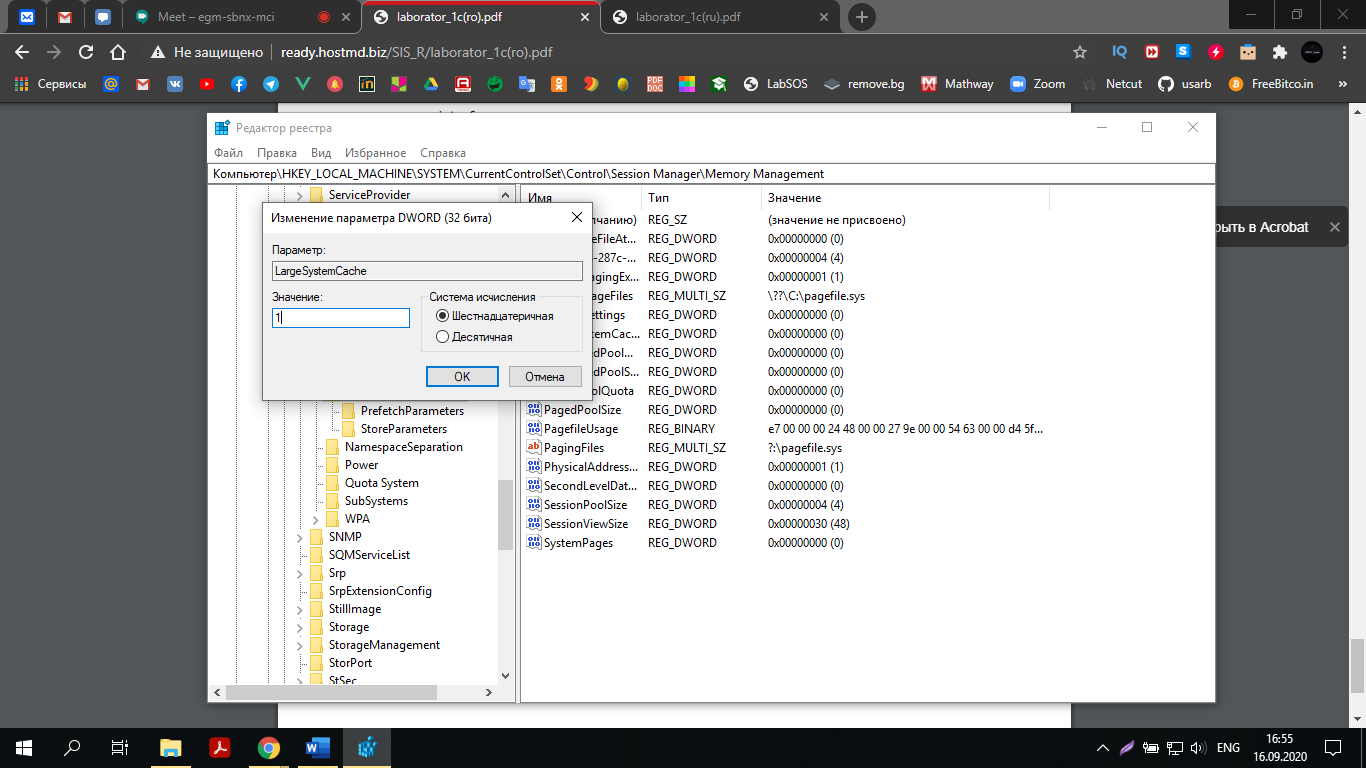


18) Opriți conținut de indexare partițiile pe disc și prefetcher pentru SSD-drive-uri.

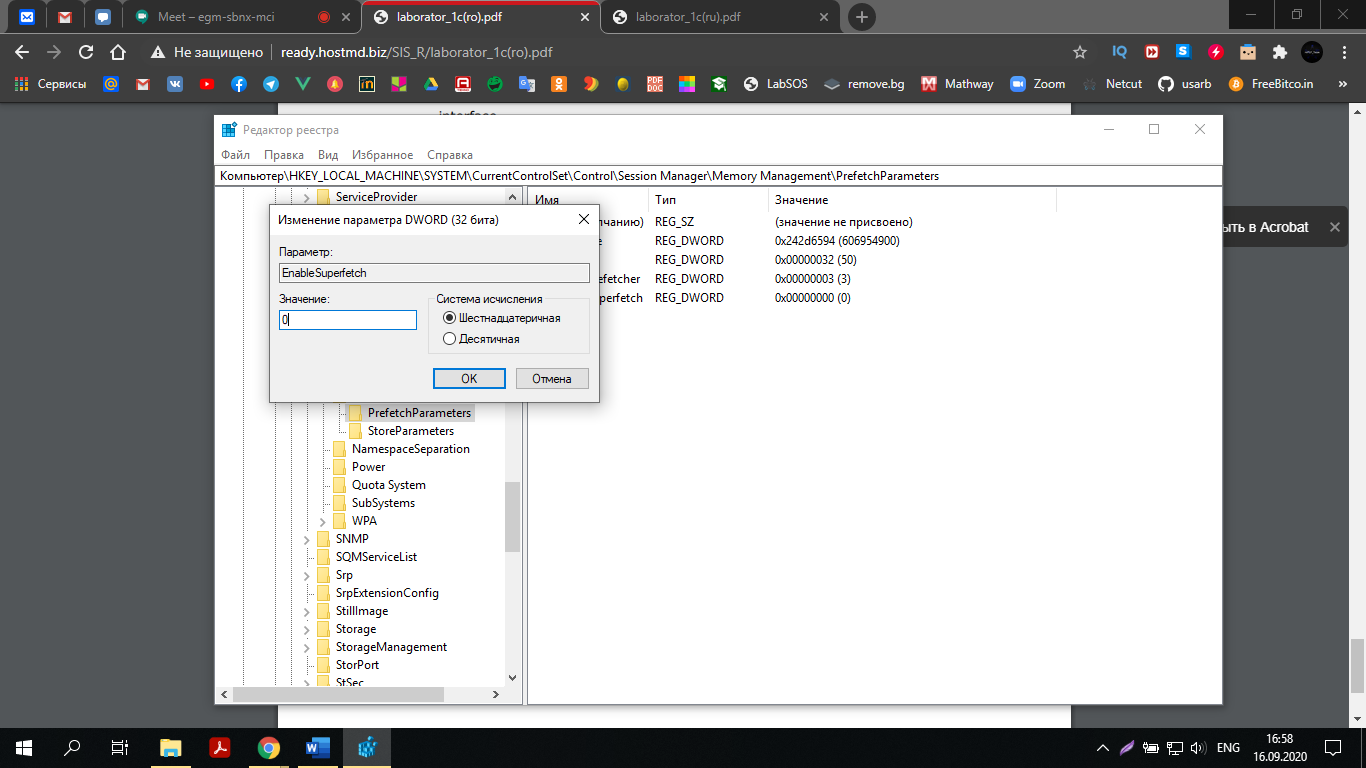
Windows Registry Editor Version 5.00

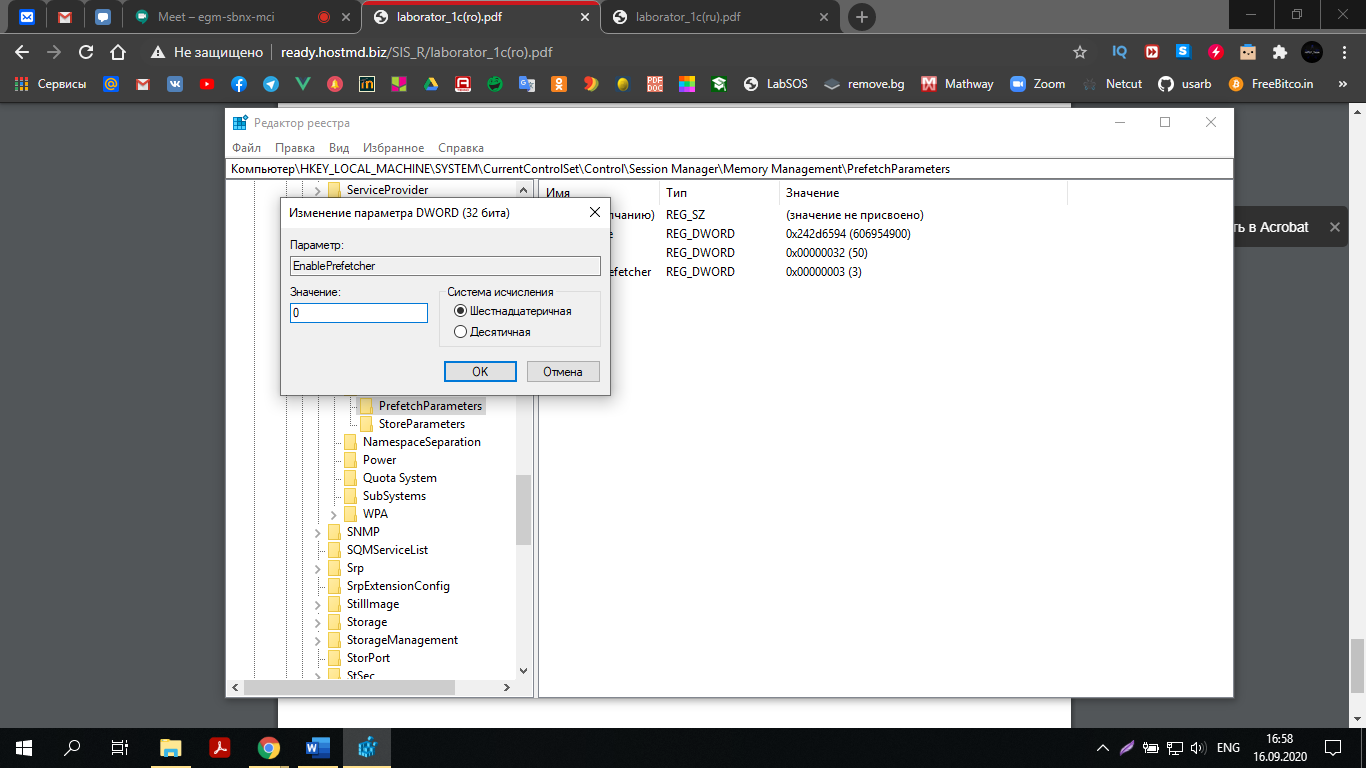
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\ Control\Session Manager\Memory Management] "DisablePagingExecutive"=dword:00000001 "LargeSystemCache"=dword:00000001



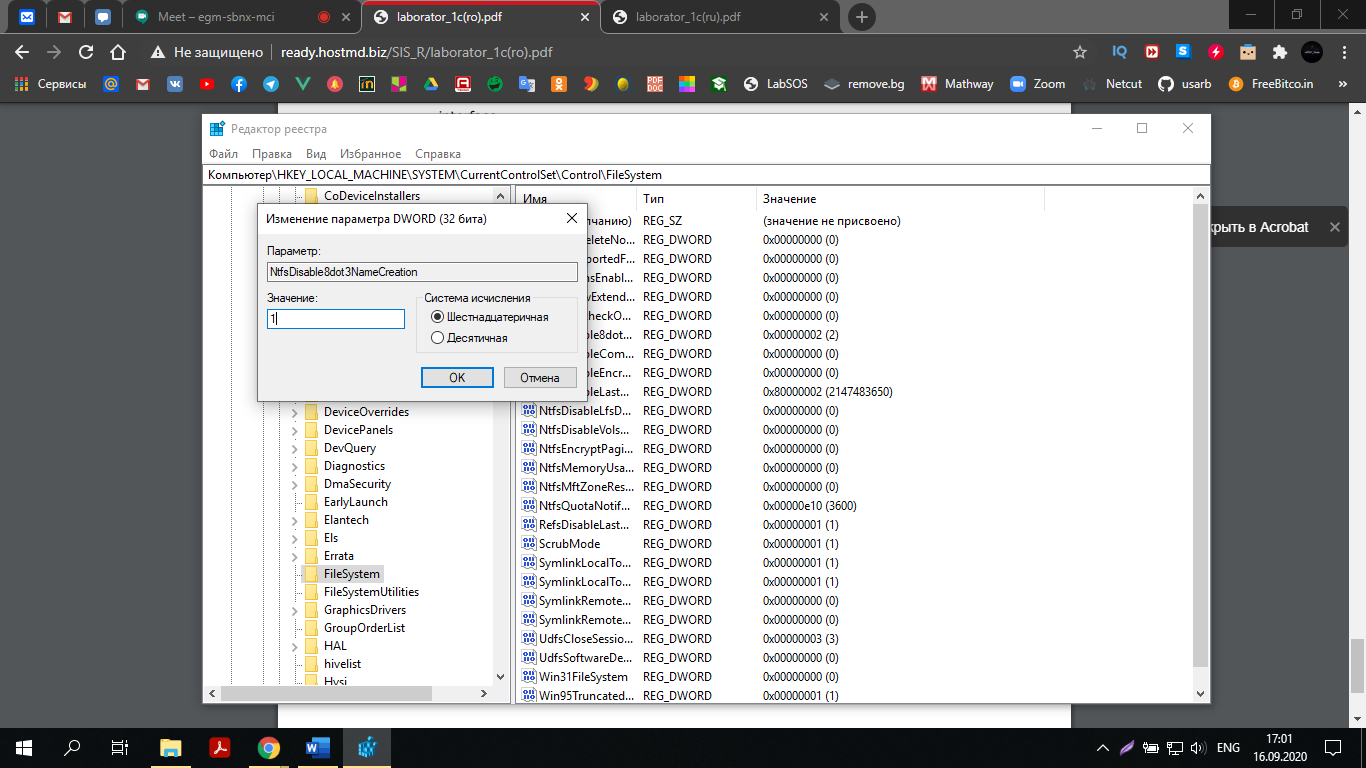


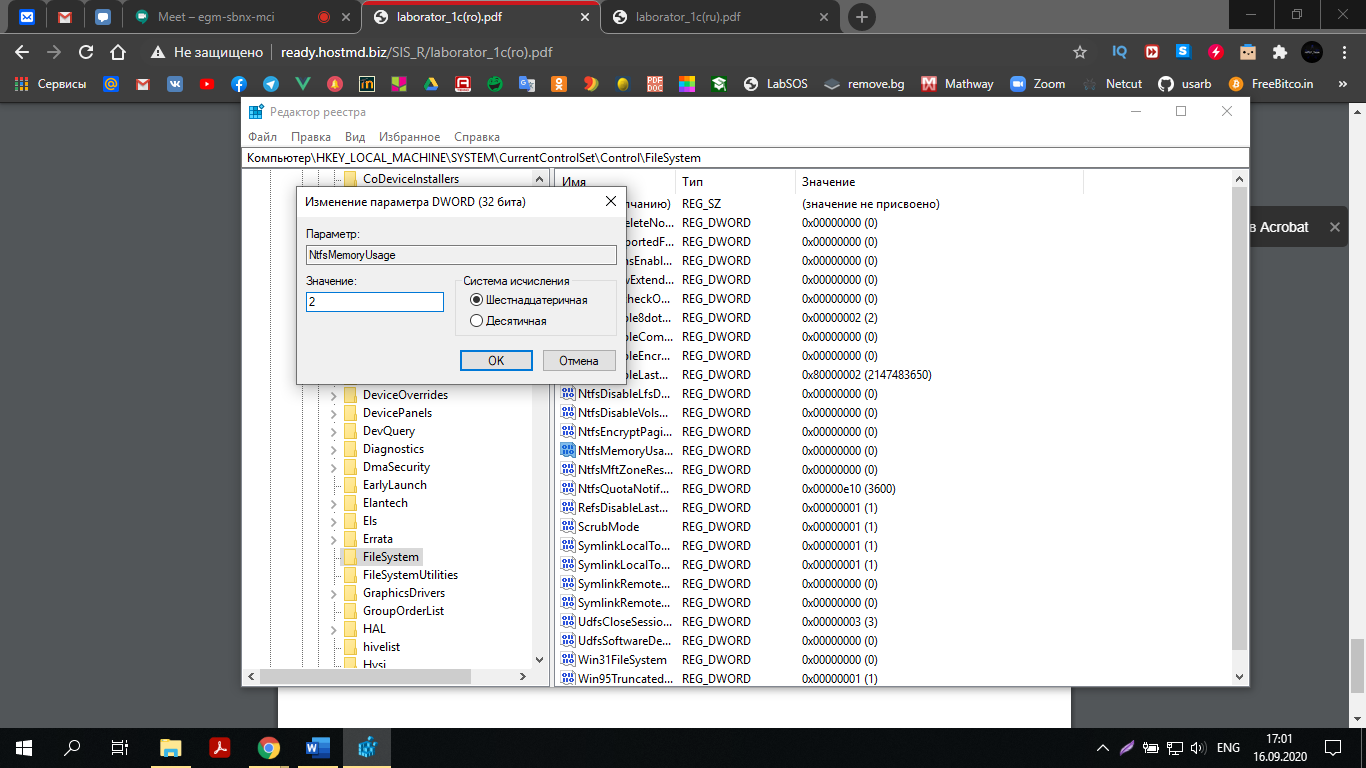
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\ Control\Session Manager\Memory Management\PrefetchParameters] "EnableSuperfetch"=dword:00000000 "EnablePrefetcher"=dword:00000000





[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\ Control\FileSystem] "NtfsDisable8dot3NameCreation"=dword:00000001 "NtfsMemoryUsage"=dword:00000002





[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction] "Enable"="N"

--- nu am gasit, lipseste

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\OptimalLayout] "EnableAutoLayout"=dword:00000000

--- nu am gasit, lipseste.