

DWCERT-070-6

Protection from encryption ransomware
for Windows PCs and file servers



Contents

1. Specific features of encryption ransomware	3
2. Special anti-virus settings for protection against encryption ransomware	5
2.1. Configuring how Dr.Web Security Space handles malicious files	6
2.2. Configuring Dr.Web Security Space system updates	7
2.3. Configuring Dr.Web Cloud	11
2.4. Configuring the anti-virus to detect previously unknown malicious files	12
2.5. Data Loss Prevention	16
2.6. Limiting encryption ransomware's penetration capacity	18
3. Doctor Web recommendations for protecting against encryption ransomware	23
3.1. Disabling the feature that hides extensions for known file types	24
4. What to do if your files get encrypted and/or a ransom demand is made	25
4.1. Decryption utilities	25
4.2. Where ransomware files may be located	26

Additional information

Educational projects	Encryption ransomware: Threat #1 "The Dancing Men" or the Encryption Trojan Invasion
The Anti-virus Times	The category "Encrypt everything" and other issues with the hashtags #Trojan.Encoder , #encryption_ransomware , #extortion and #decryption
Leaflet	Encryption ransomware: Threat #1
Video tutorial	Configuring Data Loss Prevention
Dr.Web virus library	A description of Trojan. Encoder programs

1. Specific features of encryption ransomware

Currently, one of the biggest problems local network administrators and ordinary users come up against is encryption ransomware programs, specifically those from the Trojan.Encoder family.

*Encryption ransomware (**Trojan.Encoder**) programs search for and encrypt data on the disks of infected desktops, network attached storages and in the memory of compromised mobile devices.*

Caution! *If you receive a ransom demand, never contact the criminals. Over half of the users who pay a ransom never recover their files and lose their money.*

Caution! *Even if you pay your attacker a ransom, there is no guarantee you'll get your data back. In one incident, the criminals failed to recover the data they'd previously encrypted and told their victims to contact Doctor Web's technical support service.*

The first ransomware programs of the Trojan.Encoder family emerged in 2009. The next five years saw a 1,900% increase in just the number of basic modifications alone, and currently the Trojan.Encoder family includes several thousand modifications, with at least 10 new samples arriving at the Dr.Web anti-virus laboratory on a daily basis. Encryption ransomware targets mobile devices too.

Usually encryption ransomware programs search computers and/or networks for files whose names have certain extensions (such as *.mp3, *.doc, *.docx, *.pdf, *.jpg, *.rar) and encrypt them. Individual members of the family can also encrypt other types of files.

Restoring files compromised by the Trojans is no easy task. Keys used in certain encryption routines can be brute-forced, but the ransomware often uses the most tamper-proof encryption methods. Deciphering files compromised by some ransomware programs ([Trojan.Encoder.567](#)) takes months of continuous decryption. And, data corrupted by certain Trojans ([Trojan.Encoder.283](#)) can't be decrypted at all.

Cracking the key to decrypt data encrypted by Trojan.Encoder.741 would take 107,902,838,054,224,993,544,152,335,601 years.

The specific approach adopted by criminals developing encryption ransomware makes programs of this kind particularly dangerous. During the development phase, criminals test their programs against all relevant anti-virus solutions to ensure that the malicious software can't be detected until it gets analysed in anti-virus laboratories and the corresponding virus definition updates are released.

The Dr.Web anti-virus successfully removes all known versions of encryption ransomware and can even disarm programs that haven't yet been analysed by an anti-virus laboratory. The technologies used in Dr.Web products make it significantly more difficult for hackers to create new malware species that can't be detected by Dr.Web.

Dr.Web Katana can enhance the security of machines running other conventional anti-viruses (not Dr.Web).

Important! *No anti-virus program can provide continuous protection against malware that has not yet been identified, without the help of additional security tools (such as office control).*

More information about encryption ransomware can be found at http://antifraud.drweb.com/encryption_trojs.

2. Special anti-virus settings for protection against encryption ransomware

An unknown encryption Trojan can get into a system via spam (it can be attached to a message or downloaded using a link), IM messages (also containing a download link) or from an infected site or flash drive. The infection process can be unobtrusive—modern malicious programs are designed to operate covertly, right up until files get encrypted and the program can display a ransom demand.

Important! *If your business partners and friends are careless about protecting their personal information, an email containing encryption ransomware that appears to come from an acquaintance or a well-known institution such as a bank or tax office may find its way to your inbox. Moreover, the message may be addressed specifically to you!*

1. If unknown Trojan.Encoder programs get onto a computer, they will only be detected and removed once the next virus database update has arrived. That's why virus databases should be updated as often as possible—at least once an hour.
2. If your computer is connected to the Internet, enable the Dr.Web Cloud component (available in **Dr.Web Security Space** (Windows) and in **Dr.Web Desktop Security Suite** (Windows) under the comprehensive protection license as well as in **Dr.Web Katana**). This will enable Dr.Web to detect new malware even sooner because the anti-virus will be acquiring needed information before it gets updated.
3. Criminals craft thousands of new encryption Trojans daily, and there is no guarantee that a conventional anti-virus, which uses the signatures located in its virus databases to detect them, will be able to do so at the moment of intrusion. The **proactive protection module** will compare the behaviour of launched programs with that of encryption ransomware in real time, allowing unidentified members of the Trojan.Encoder malware family to be detected.

Important! *The Parental Control and Preventive Protection can make it much more difficult for malware to penetrate a system. By restricting users (and running applications) from accessing files and folders, you can ensure the integrity of your data. Even if neither the anti-virus engine nor the preventive protection technologies recognise a malware program, it won't be able to start or will be detected as soon as it attempts to access one of the system's protected elements.*

4. Unfortunately, even a behavioural analyser, which enables the anti-virus to detect even unknown encryption ransomware iterations, can't always prevent encryption—while Dr.Web is analysing the behaviour of a suspicious process, the Trojan can encrypt up to ten files. To keep your data safe, configure the Data Loss Prevention component of Dr.Web Security Space. It is also included in **Dr.Web Desktop Security Suite** (Windows) under the comprehensive protection license.




Even if you already back up your data for better security, using the Data Loss Prevention feature is still recommended because it will help preserve critical data in a more expeditious manner. Unlike conventional backup programs, Dr.Web creates backups and protects them from intruders

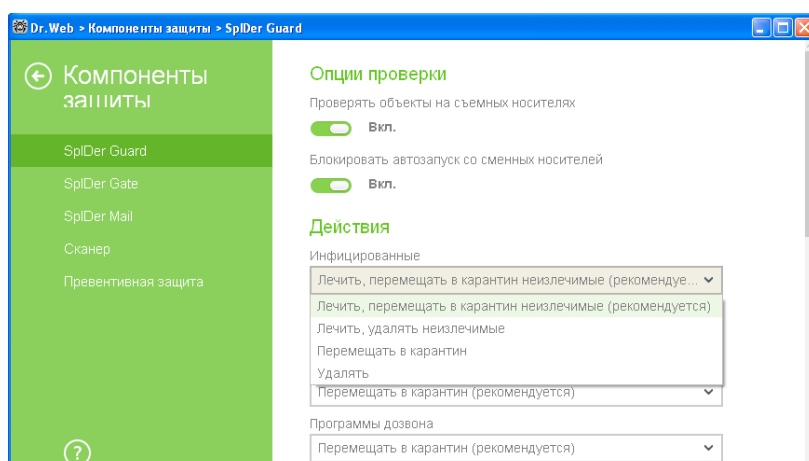
Important! Since **Dr.Web Security Space** and **Dr.Web Desktop Security Suite** have the same features that protect against encryption ransomware, Dr.Web Security Space settings will be provided as an example.

2.1. Configuring how Dr.Web Security Space handles malicious files

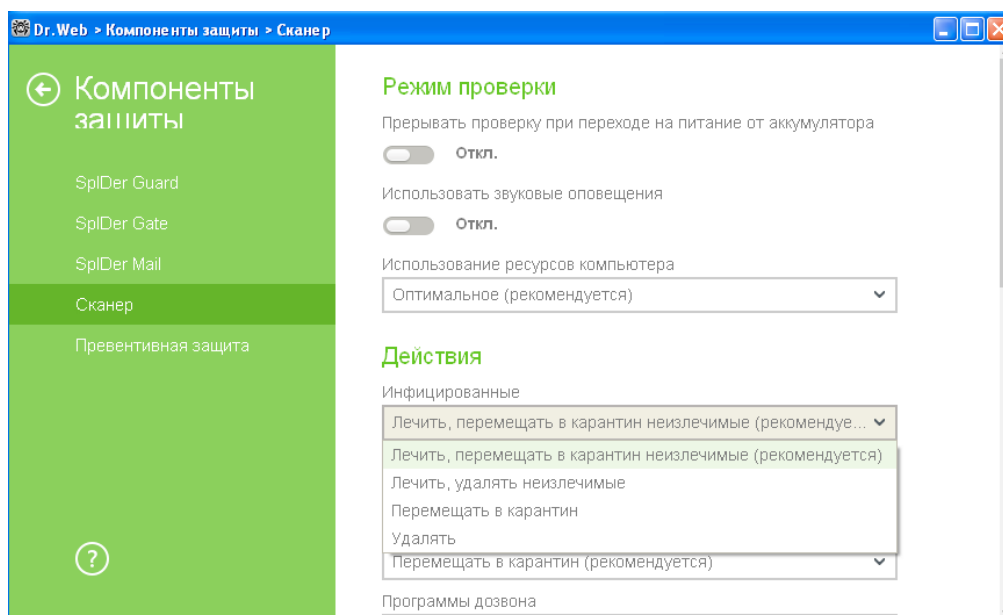
To restore data from encrypted files, it is best to have on hand the malicious file that was used to corrupt them. If unknown Trojan.Encoder programs get onto a computer, they will only be detected and removed once the next virus database update takes place. That's why, if detected, these files should be moved to the quarantine instead of deleted.

Important! The anti-virus scanner can alter certain system properties. This in turn can make further analysis of the computer incident impossible and destroy the evidence. We recommend that you follow established procedures to create a disk image and use it to restore your data.

Click on the  icon in the system tray, and in the context menu, select the  Administrator Mode, and then click on the gears icon  (Settings). In the Settings window, select **Protection Components** and then choose **SpIDer Guard**.






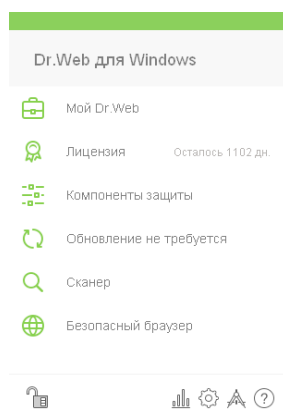
Similar settings should be used for anti-virus scanning. The settings can be adjusted in the **Scanner** tab in the same window.



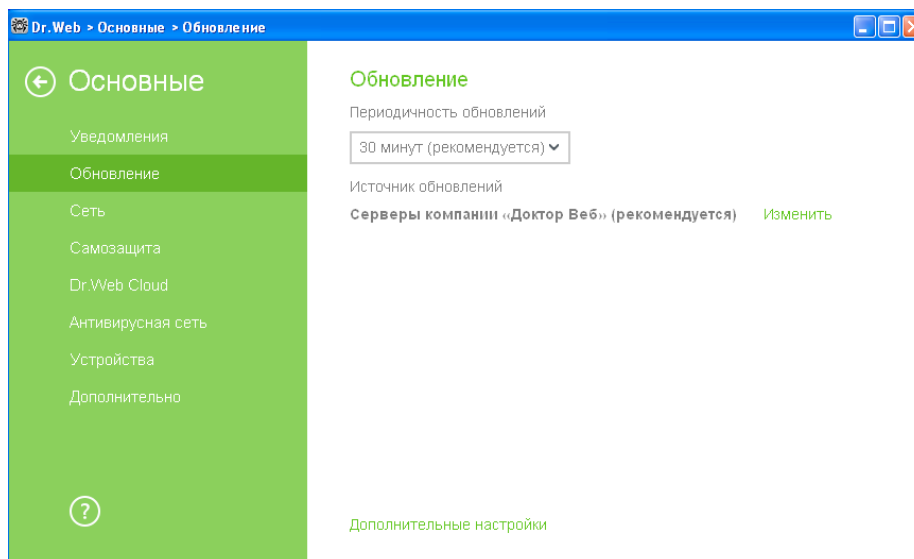
Important! Do not delete the quarantined objects because in some cases malicious files may contain keys that can help decrypt files.

2.2. Configuring Dr.Web Security Space system updates

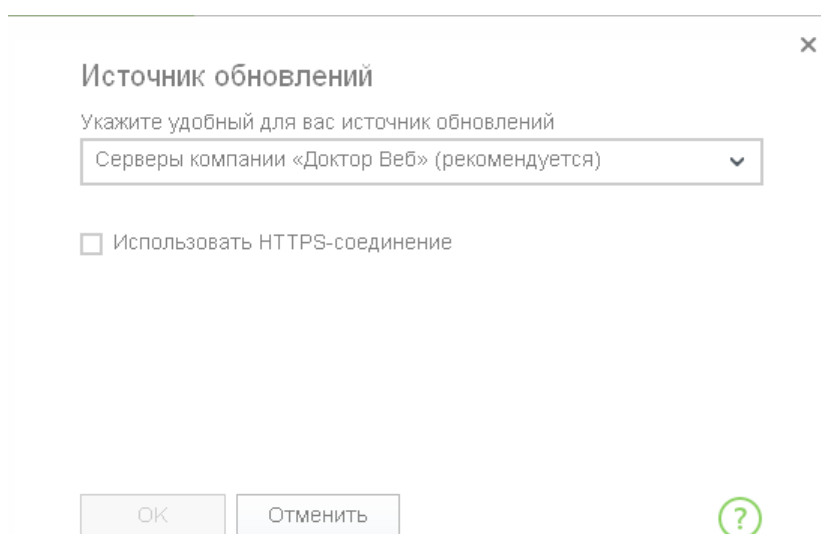
Click on the icon in the system tray, and in the context menu, select the icon,  and then click on the icons  and .



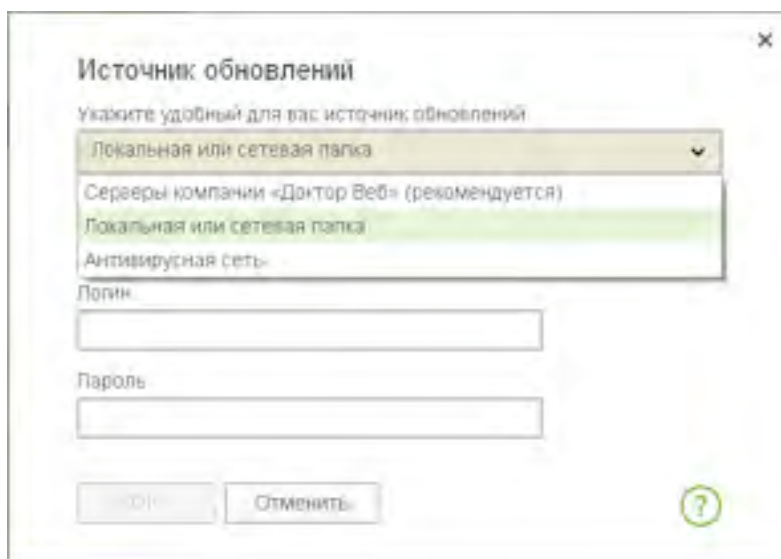
In the next window that opens, select **Settings** → **Main** → **Update**.



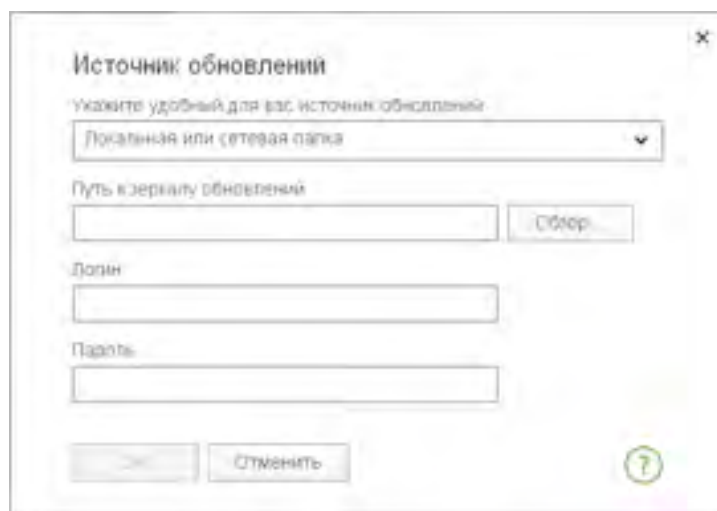
By default, the anti-virus retrieves updates from Doctor Web's servers. To change the update source, click **Change**.



Three options are available:

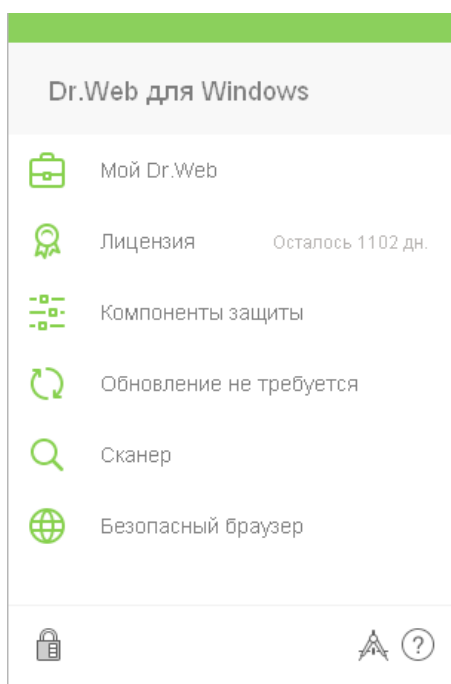


If updates are to be retrieved from a local directory, specify the directory and its access parameters.

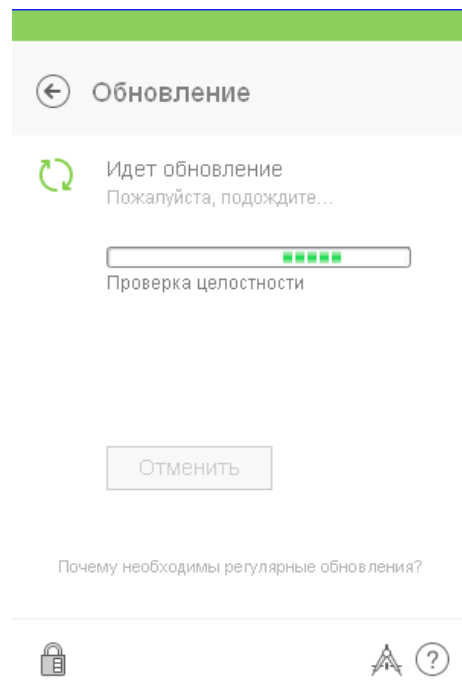
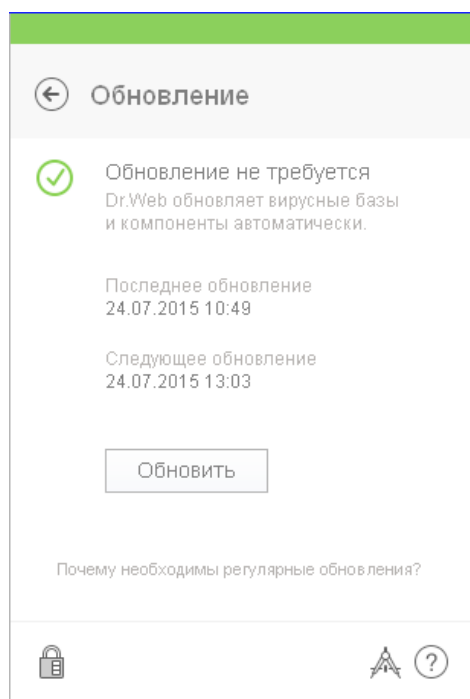


If you intend to retrieve updates from an anti-virus server, configure updating in a similar fashion.

To update the anti-virus or to check the update status, click  in the menu and select .

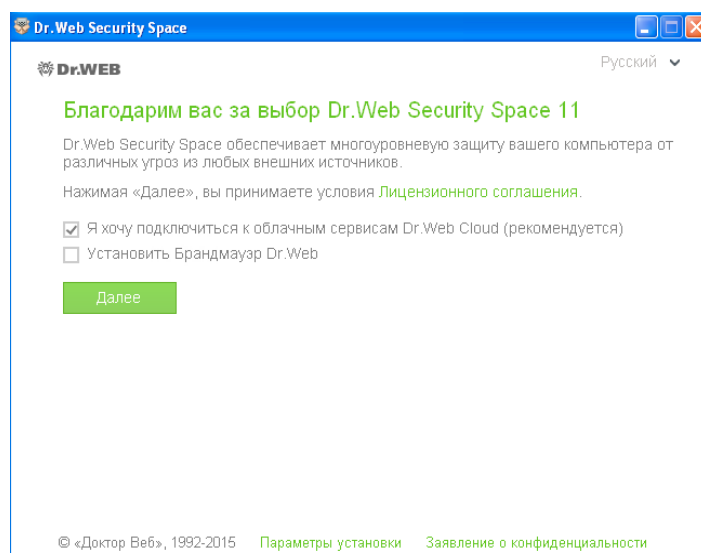





To update the software manually, click **Update**.

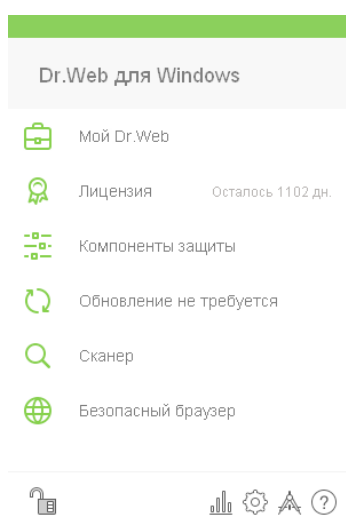


2.3. Configuring Dr.Web Cloud

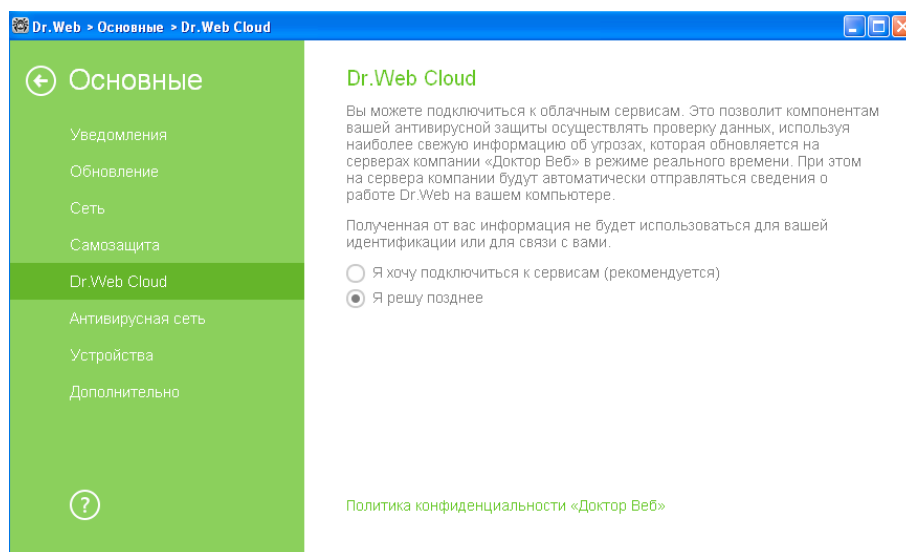
You will be prompted to use Dr.Web Cloud during the Dr.Web Security Space installation process. To enable this feature, do not clear the **I want to connect to services** checkbox. After the installation, reputation queries for each scanned object will be sent automatically and won't consume any of the protected computer's resources.



If Dr.Web Cloud wasn't enabled during the installation, click on the icons  and . Then click on the icon .



In the Settings window, select **Main** → **Dr.Web Cloud**.



In the subsequent window, select **I want to connect to services**.

2.4. Configuring the anti-virus to detect previously unknown malicious files

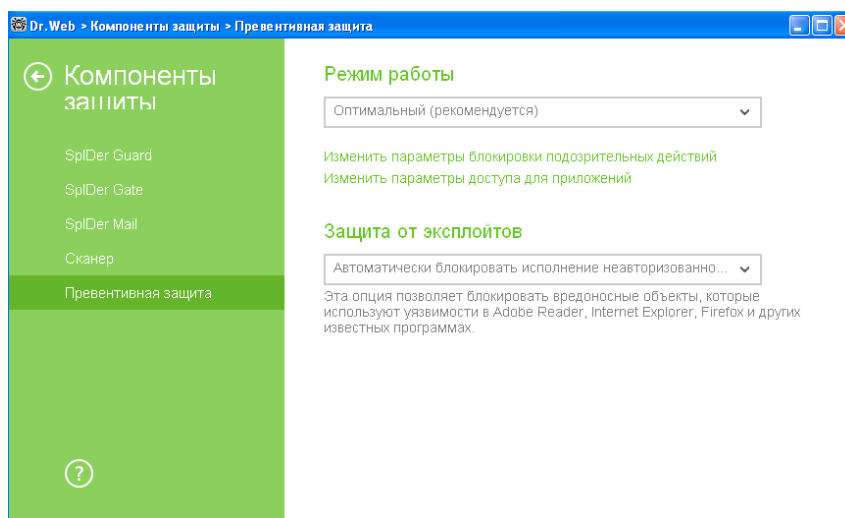
The proactive protection module will compare the behaviour of launched programs with that of encryption ransomware in real time, allowing unknown members of the Trojan.Encoder malware family to be detected.

Previously unknown programs can be detected during background scanning of running processes as well as with scheduled and on-demand anti-virus scans.

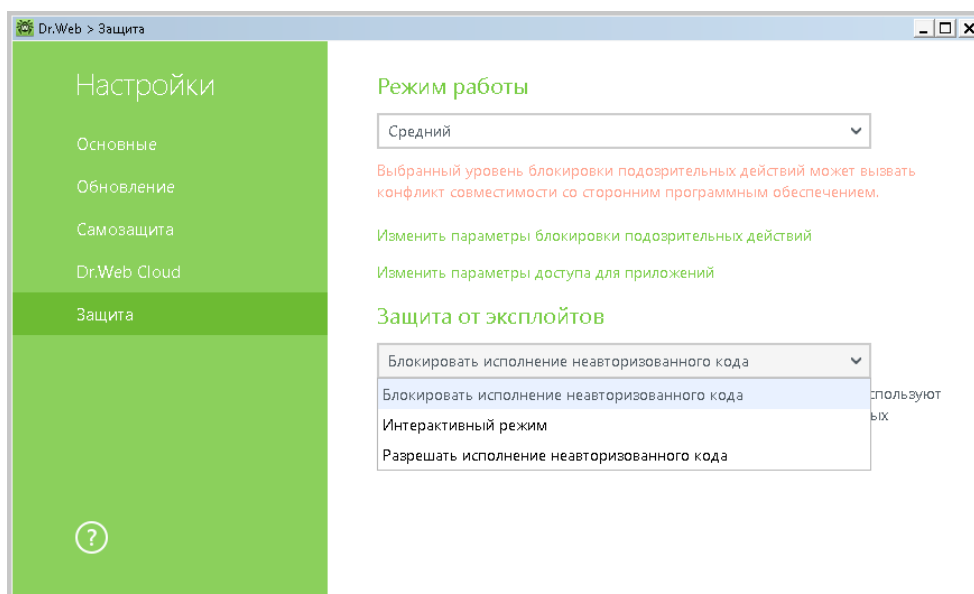
The Dr.Web anti-rootkit API facilitates background scanning and the neutralisation of active threats. The routines continuously reside in the memory and search for threats in the following critical Windows system areas: Start-up objects, running processes and modules, RAM, the VBR and MBR, and the system BIOS. If threats are detected, Dr.Web can notify the user about the danger, cure the infection, and block malicious activities.

To configure the proactive protection feature, click on the  icon in the system tray, and in the context menu, click on the icons  and .

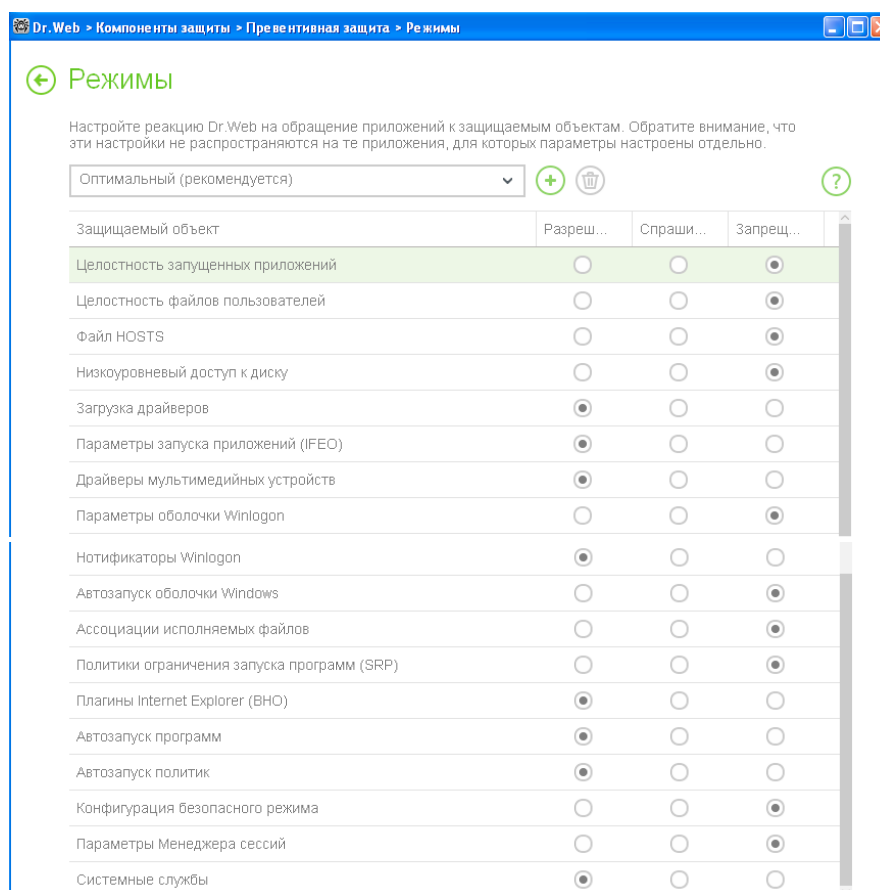
In the Settings window, select **Protection Components** and then choose **Preventive Protection**.



Important! In Dr.Web Katana, the Preventive Protection component has a different name:



To configure the anti-virus's response to the actions of third-party applications that can infect your computer, adjust the suspicious activity blocking level. The preventive protection enables the anti-virus to maintain control over changes in all critical areas of Windows. To change the preventive protection settings, click **Change level of suspicious activity blocking**.



In the default **Optimal** mode, the automatic modification of system objects—activity that would clearly indicate malicious activities are occurring in the system—is disabled. Low-level access to the disk is also disabled to protect the system from bootkits and blocker Trojans that infect the Master Boot Record. So that malware cannot prevent the anti-virus from being updated via the Internet or block access to anti-virus developers' sites, modifying the HOSTS file is not allowed.

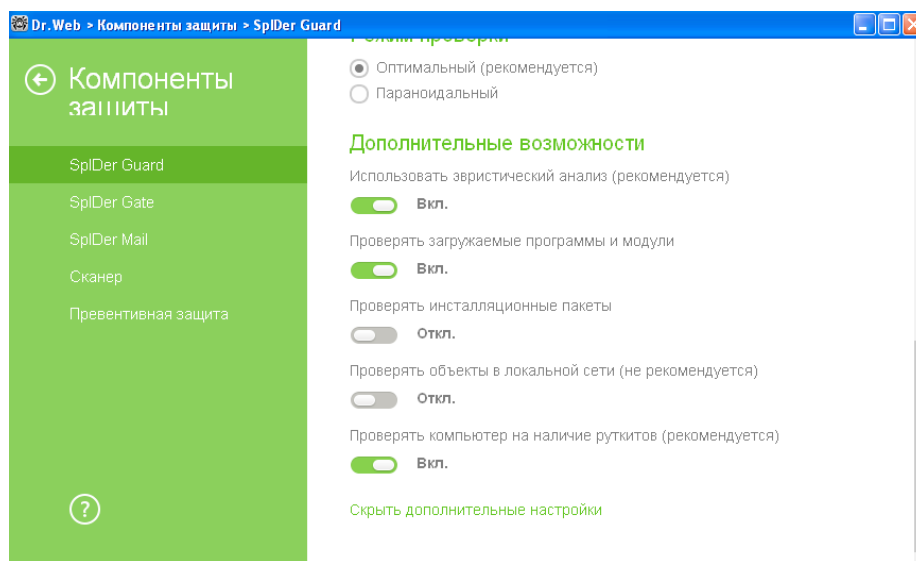
If the threat of infection increases, raise the protection level to **Medium**. In this mode, access to objects that can potentially be used by malware is also blocked.

Important! In this protection mode, compatibility issues can arise between Dr.Web and third-party programs that use protected Windows Registry branches.

If you want Dr.Web to maintain full control over critical Windows areas, you can increase the protection level to **Paranoid**. In this case, the prompt mode is used for loading drivers and automatically launching programs.

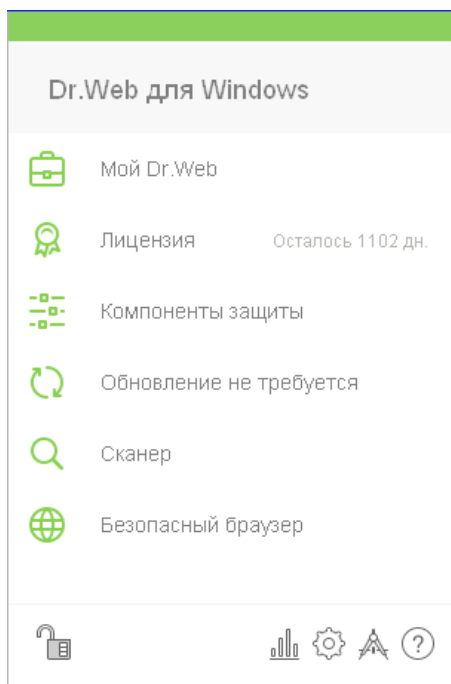
To adjust the preventive protection, set the desired level of access to the protected objects. The mode will be switched to **User-defined** automatically. In the User-defined mode you can adjust the anti-virus's responses to certain actions that can result in your computer becoming infected.

To enable anti-rootkit scanning, in the Settings window, select **Protection components** → **SplDer Guard**. In the next window, click **Advanced settings**. By default, the option to scan the system for rootkits is enabled.

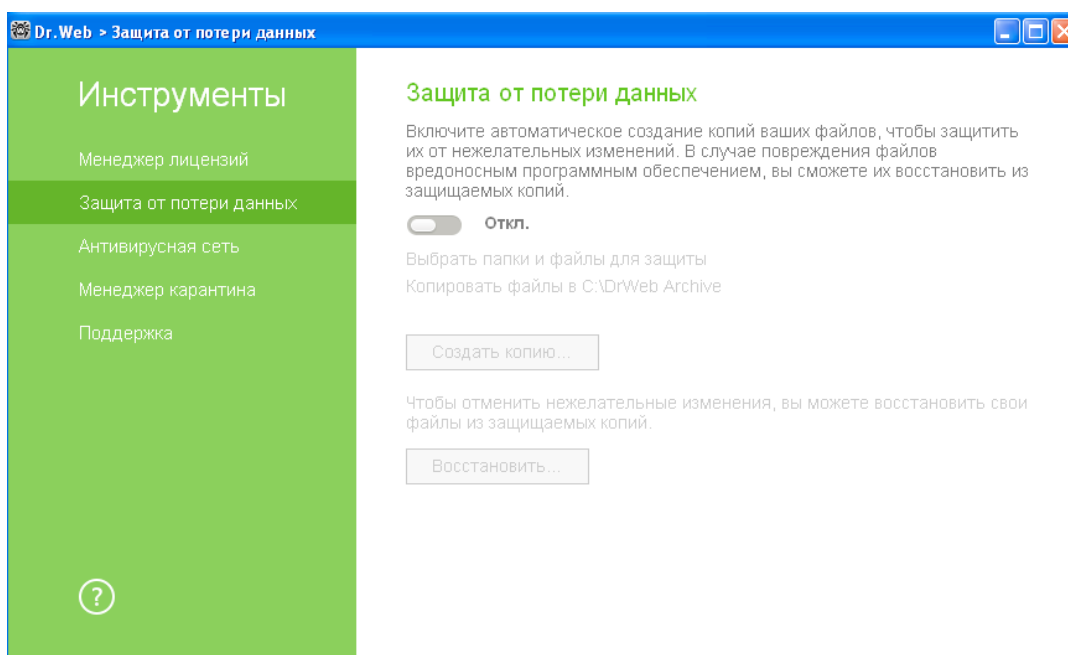


2.5. Data Loss Prevention

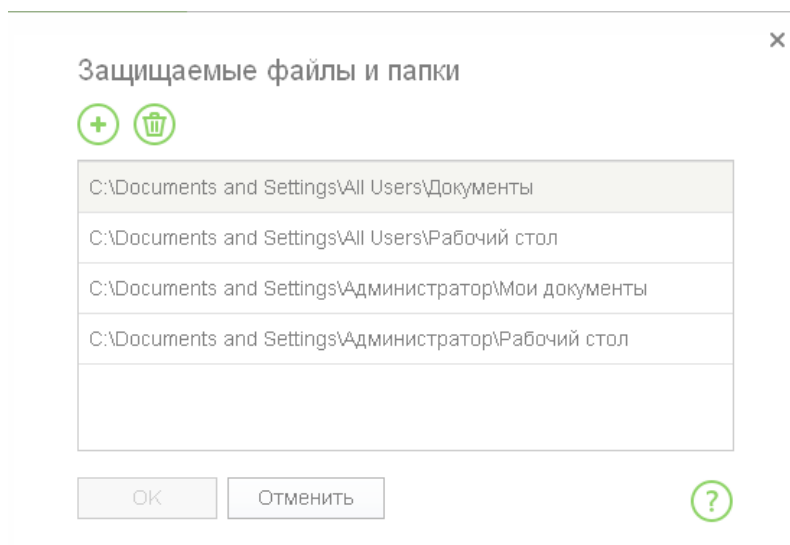
To configure the Data Loss Prevention feature, click on the icon  in the system tray. Then, in the next menu, click on the icons  and .




In the next window, select Data Loss Prevention and enable automatic backups.

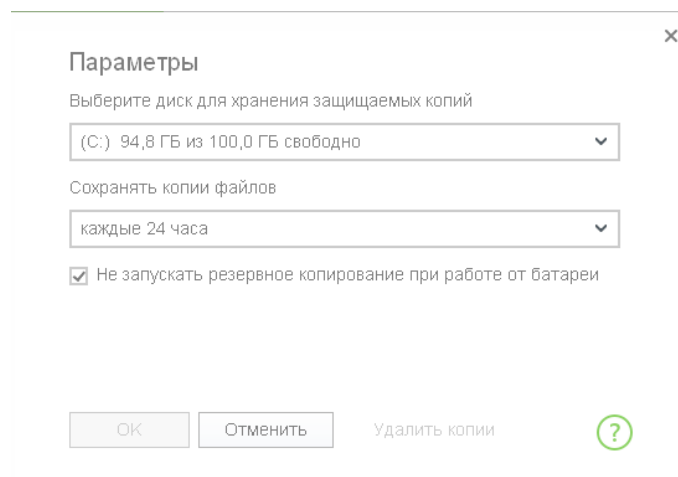


After that you will need to specify the files and folders that are to be backed up.



To add files and folders onto the list, click on the icon  and specify the files and directories to be protected.




Select **Copy files...** to specify how often backups will be made and where they will be stored.

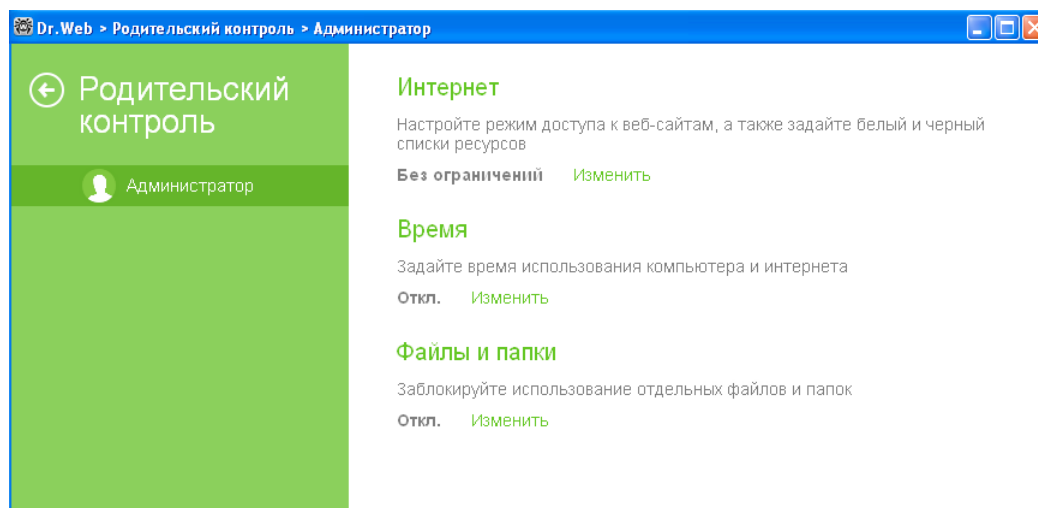


2.6. Limiting encryption ransomware's penetration capacity

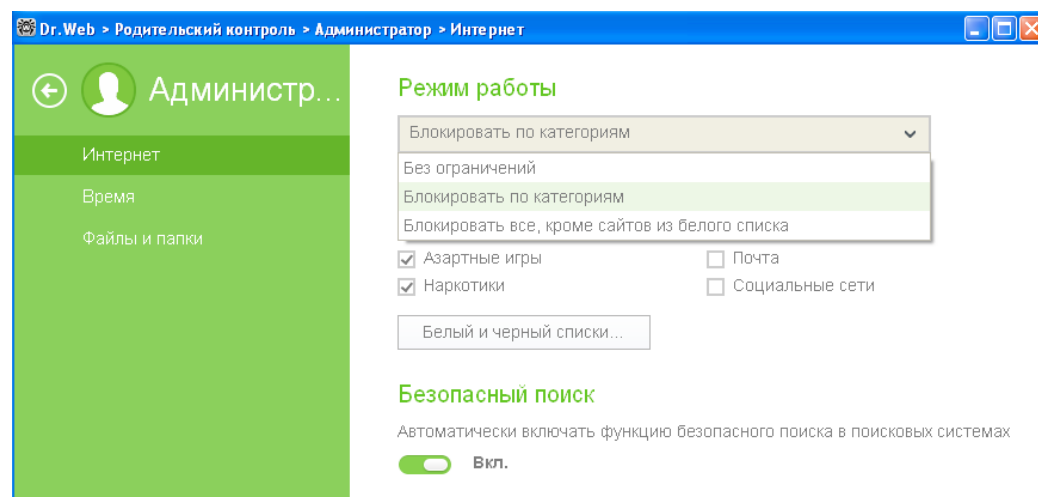
An encryption Trojan can get into a system via spam (it can be attached to a message or downloaded using a link), IM messages (which also contain a download link) or from an infected site or a flash drive. To lower the infection risk, use an anti-spam and restrict access to potentially dangerous sites and removable data storage devices.

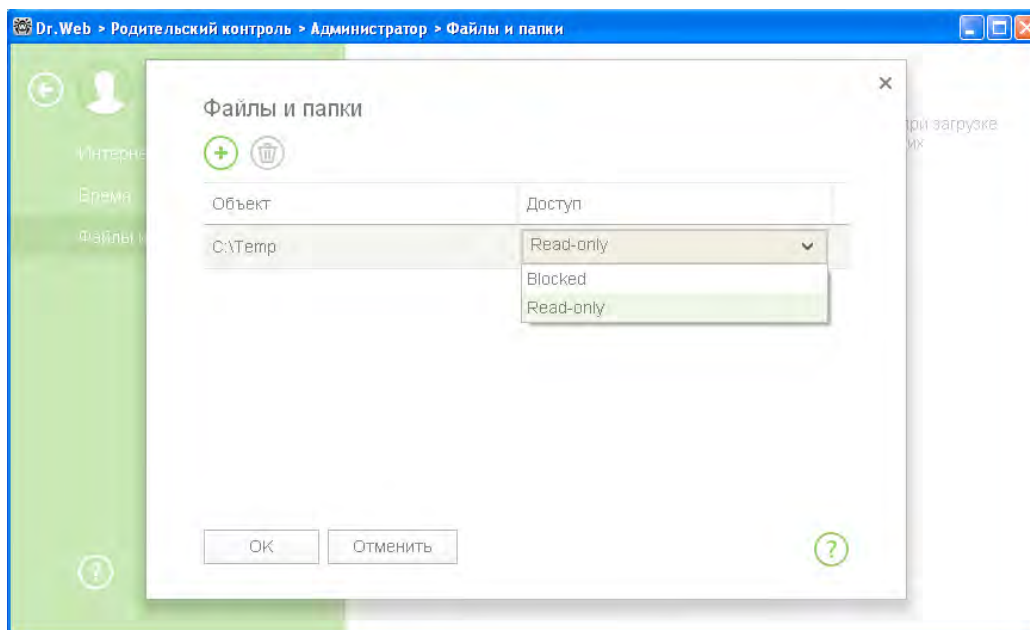
This course doesn't cover anti-spam configuration because the anti-spam becomes operational by default, without any additional tuning, as soon as Dr.Web Security Space is installed.

To restrict access to certain sites, files, and folders, click on the icons  и  .
Then click on the icon  , and in the Settings window, select **Parental Control**.



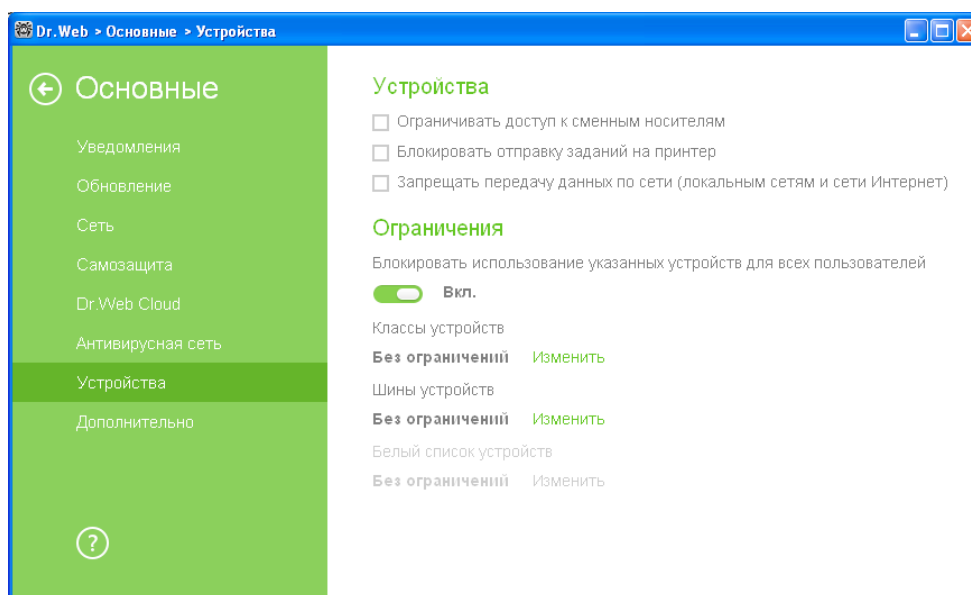
In the next window, select the user account for which you want to set restrictions.



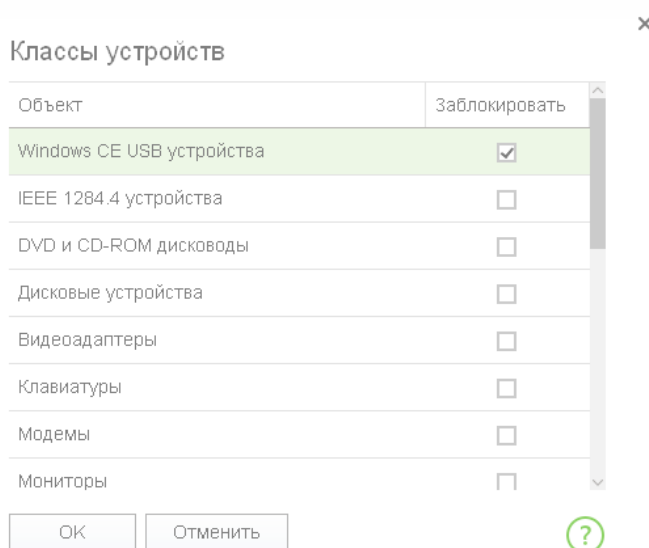


By default, there are no restrictions.

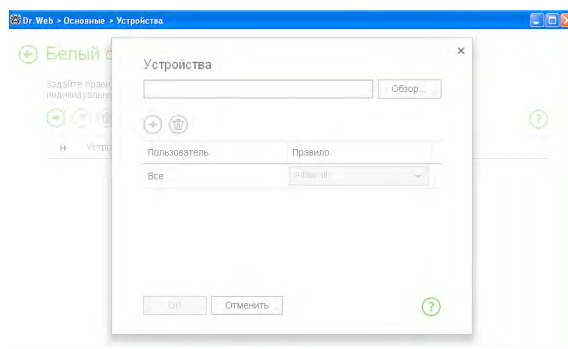
To restrict access to removable media, in the **Settings** window, select **Main → Devices**.



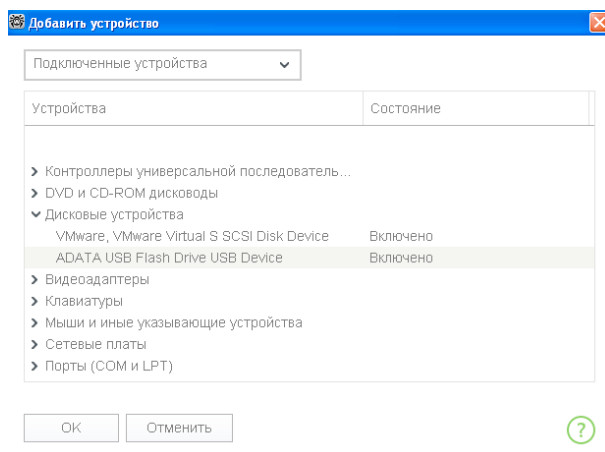
In this window, select **Restrict access to removable media**. Then click Change for the device classes, and select the desired device classes.



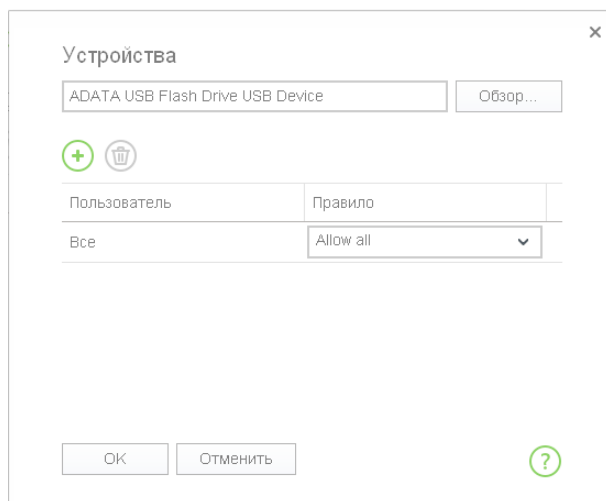
After that, you will be able to configure the **White list**. If you only want devices on the white list to be accessible, click **Change** → .




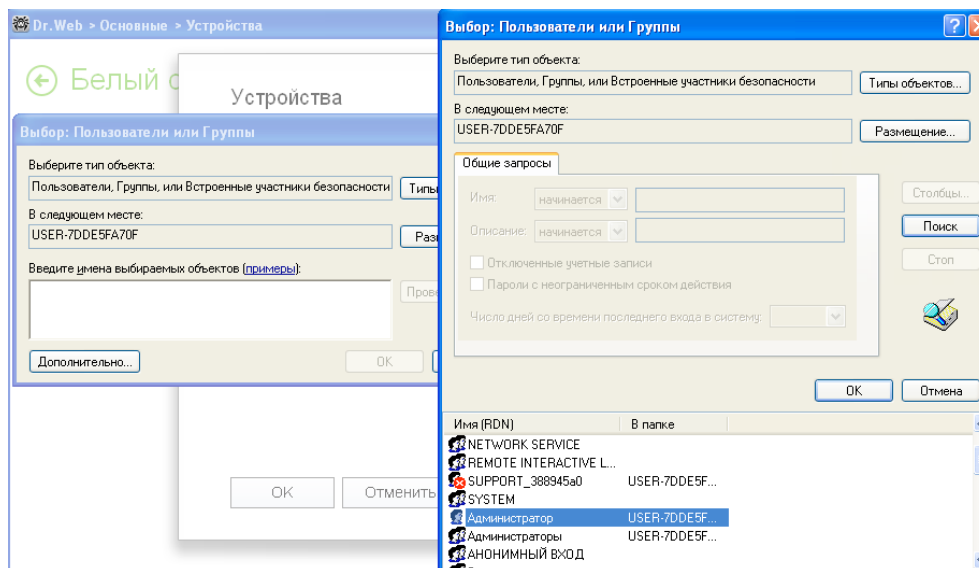
Then click Change for the device classes, and select the desired device classes.



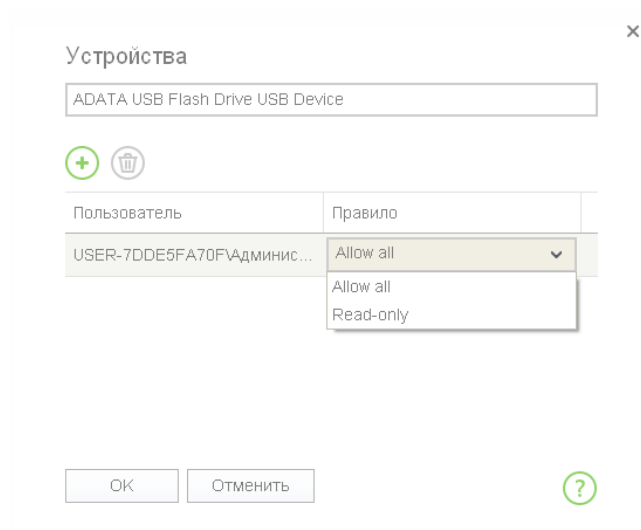
Press **OK** to confirm your choices.



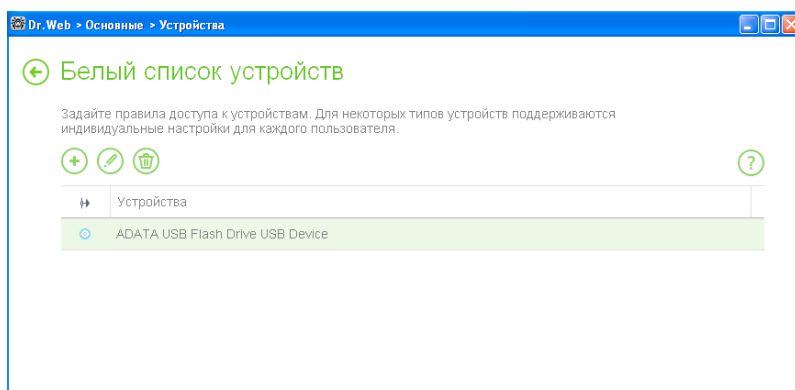
If you want to grant specific users access to particular media, click on the icon  and select the user accounts for which you need to grant access.



Specify permissions for the device.



Confirm your selection.



3. Doctor Web recommendations for protecting against encryption ransomware

Dr.Web statistics show that 90% of the time, users launch encryption ransomware themselves.

- Never give your consent when you are prompted to open attachments or a document (these are usually specially generated doc and pdf files; but, they can also be placed into .zip, .rar, .7z and .cab archives since users often disable the option to scan compressed files in order to boost system performance).
- Use back-up solutions (back up files or the entire system). It is not recommended to create backups by copying files manually, or to store backups on the computer itself. It is not recommended to store backups on a different hard drive or in a network location that is accessible from a local computer. Instead, use removable media and/or cloud storage, and encrypt backups. Thus, files are protected not only from ransomware but also from hardware failures.

Important! *Before you create a backup, make sure that the files haven't been encrypted and won't replace unencrypted versions of the files.*

Windows Vista and later Windows versions incorporate a system protection service that creates copies of files and folders when backups and system restore points are created. By default, the service is enabled only for the system drive.

Important! *The service won't protect the system from encryption ransomware, but the Trojans can turn off the service and destroy earlier backups.*

- Do not open email attachments from unknown senders. In most cases, encryption ransomware spreads via email attachments. Criminals lure users into opening attachments or links.
- If your data has been compromised by encryption ransomware, never use decryption programs, change file name extensions or take other steps without appropriate guidance. Your actions can result in permanent data loss so that even a special decryption utility won't be able to find the files and restore them.
- Disable the option to hide extensions for known files types (see section 3.1. below). If file extensions are hidden, you won't be able to determine actual file types.

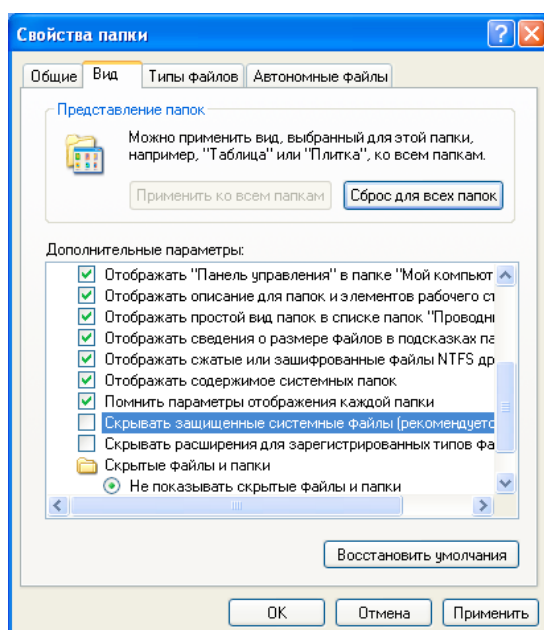
- Use only legal copies of software.
- Promptly install operating system security updates as well as updates for all the applications installed on your computer.
- Configure access permissions for all user accounts in the system, for user data and network folders. Otherwise, if the system gets infected, all user documents will be encrypted, including those stored in network folders.

More information about the actions one can take if a system gets infected by encryption ransomware can be found here: <http://legal.drweb.com/encoder>.

3.1. Disabling the feature that hides extensions for known file types

To make Windows display extensions for all files types:

- **Windows XP:** In the **Start** menu, select **Control Panel** → **Folder Options** and clear the checkbox **Hide extensions for known file types**.



- **Windows 7:** Press left Alt on the keyboard. In the next menu, click **Tools** → Folder Options; open the **View** pane, and in the advanced list, clear the checkbox **Hide extensions for known file types**.
- **Windows 8/8.1:** Open any folder or start Windows Explorer by pressing the Windows key + E. In the Explorer main menu, select View and check the box File name extensions—with this option enabled, file extensions will be displayed in all windows; otherwise extensions are hidden.

4. What to do if your files get encrypted and/or a ransom demand is made

To increase your chances of successfully recovering your encrypted data, never do any of the following:

- Change file name extensions for encrypted files.
- Reinstall Windows.
- Use any data recovery/decryption programs on your own without the assistance of Doctor Web's technical experts.
- Delete/rename any files (including temporary files) and applications.
- If you initiated a virus scan, do not take any irreversible actions such as curing/removing the malware.

4.1. Decryption utilities

Special utilities provided by Doctor Web technical support upon request can decrypt files compromised by ransomware. Unfortunately, so many encryption malware programs appear every day that it's impossible to create decryption utilities for each of them. Therefore, if your files have been encrypted by a Trojan that has yet to be identified, you can order the decryption service (https://support.drweb.ru/new/free_unlocker/?keyno=&for_decode=1). The service is available free of charge for users who have purchased commercial Dr.Web software.

If you require the decryption service, please [send](#) Doctor Web at least 3-5 encrypted files of various formats. A description of the infection incident, including the ransom demand text, can help decrypt the data. If you know which file you launched to enable the Trojan to compromise your data, attach it to your request to the Dr.Web technical support service.

 **Important!** *Create copies of encrypted files before you launch the utility.*

4.2. Where ransomware files may be located

If you have discovered a suspicious file and you believe that by launching it, your computer could become infected and your files encrypted, send the suspicious file to the virus laboratory for analysis. Paths to locations in which files of this kind can be found are as follows:

APPDATA	Windows NT/2000/XP: System drive:\Documents and Settings\%UserName%\Application Data\%USERPROFILE%\Local Settings\Application Data Windows Vista/7/8: Drive:\Users\%UserName%\AppData\Roaming\ %USERPROFILE%\AppData\Local
TEMP (storage for temporary files)	%TEMP%*.tmp %TEMP%*.tmp\ %TEMP%* %WINDIR%\Temp
Internet Explorer temporary directory	Windows NT/2000/XP: %USERPROFILE%\Local Settings\Temporary Internet Files\ Windows Vista/7/8: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\ ..\temporary internet files\content.ie5\ ..\temporary internet files\content.ie5*\
Desktop	%UserProfile%\Desktop\
Recycle Bin	Drive:\Recycler\ Drive:\\$Recycle.Bin\ Drive:\\$Recycle.Bin\s-1-5-21-????????- ????????-????????-1000 (? -- 0-9)
System directory	%WinDir% %SystemRoot%\system32
My Documents	%USERPROFILE%\My Documents\ %USERPROFILE%\My Documents\Downloads
Browser download directory	%USERPROFILE%\Downloads
Autorun directory	%USERPROFILE%\Start Menu\Programs\Startup

Important! Trojan.Encoder files can be found in other directories too.

About Doctor Web

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web products have been in development since 1992. The company is a key player on the Russian market for software that meets the fundamental need of any business – information security.

Doctor Web is one of the few anti-virus vendors in the world to have its own technologies to detect and cure malware. The company has its own anti-virus laboratory, a global virus-monitoring service, and a technical support service.

Doctor Web's strategic goal upon which the efforts of its entire staff are focused is to create superlative anti-virus software that meets all the current demands of this market segment, and to develop new technologies that allow users to be fully armed against all types of computer threats.

Training

[My Dr.Web Training Portal](#) (registration required)
[Courses for engineers](#) | [Courses for users](#) | [Brochures](#)

Education

[The Anti-virus Times](#) | [WebIQmetr](#) | [Brochures](#)

Contacts

Headquarters Doctor Web Ltd.
125040, Russia, Moscow, 3rd street Yamskogo polya 2-12A

[Phone numbers](#)

[How to reach us](#)

[Media contacts](#)

[Doctor Web Offices outside the Russian Federation](#)

www.drweb.com | www.free.drweb.com | www.av-desk.com | www.drweb-curent.com



© Doctor Web,
2003 – 2017



Join us on social networking sites

