Doctor Web, S.L
125124, Moscú, C./ 3ª
Yamskogo Polya, edf. 2,
entrada 12A

Teléfono: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97

www.drweb.com

Proteja lo creado

Protección de estaciones de trabajo y servidores de archivos Windows contra las acciones de programas cifradores

Manual para las prácticas del curso

DWCERT-070-6

© Doctor Web, 2003 – 2015

Doctor Web, S.L
125124, Moscú, C./ 3ª
Yamskogo Polya, edf. 2,
entrada 12A

Teléfono: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97

www.drweb.com

Proteja lo creado

Versión del documento 2.0

Fecha del último cambio 02 de diciembre de 2015

Contenido

© Doctor Web, 2003 – 2015

1. ¿En qué consiste la peculiaridad (el peligro) de programas cifradores?

Hoy día uno de los problemas más importantes para los administradores de redes locales y algunos usuarios son las acciones de programas cifradores — troyanos de la familia Trojan.Encoder.

> **Los troyanos cifradores (Trojan.Encoder)** son los programas nocivos que buscan en las unidades del equipo infectado o en la memoria del dispositivo móvil los archivos de usuario, luego los cifran y demandan a la víctima un rescate por descifrarlos.

¡Atención! En caso de haber recibido una demanda de rescate— no se ponga en contacto con los malintencionados. En más de 50% de los casos, una vez pagado, Vd. no recibirá el descifrador y perderá el dinero.

¡Atención! Hasta en caso de pagar un rescate al malintencionado, eso no le dará ninguna garantía de recuperar la información. Una vez se produjo un caso, cuando los malintencionados no pudieron descifrar los archivos cifrados por ellos mismos y aconsejaron a sus víctimas contactar con el servicio del soporte técnico de la empresa Doctor Web.

Los primeros troyanos cifradores de la familia **Trojan.Encoder** aparecieron en el año 2009. Durante los cinco años siguientes, el número de sus variedades básicas se aumentó en un **1 900%**, y actualmente **Trojan.Encoder** tiene **varias miles de modificaciones** — todos los días al laboratorio antivirus Dr.Web llega una decena de nuevas muestras como mínimo. Los troyanos cifradores existen no solo para PCs (sistemas operativos MS Windows y Linux), sino también para dispositivos móviles.

Normalmente los troyanos cifradores detectan en un equipo y/o en la red local los archivos con extensiones determinadas (por ejemplo, tales como *.mp3, *.doc, *.docx, *.pdf, *.jpg, *.rar, y otros) y los cifran. Algunos representantes de la familia pueden también cifrar otros archivos.

La recuperación de archivos cifrados por un troyano no es una tarea fácil. A veces los archivos se descifran por medio de detectar las contraseñas-claves para los tipos de cifrado usados, pero con mucha frecuencia los cifradores usan los métodos más

resistentes de cifrado. Algunos virus cifradores requieren meses de descifrado continuo (Trojan.Encoder.567), y otros (Trojan.Encoder.283) no pueden ser descifrados correctamente.

> Para detectar las claves manualmente para los resultados de funcionamiento de Trojan.Encoder.741, se necesitan 10790283805422499354415233601 años.

El problema más importante vinculado con los troyanos de la familia Trojan.Encoder está vinculado con el sistema de desarrollo de los mismos usado por los malintencionados.

Durante el desarrollo se realizan las pruebas de programas nocivos creados para que los mismos no se detecten por las soluciones antivirus actuales.

Como resultado de lo cual, antes de ser analizados en los laboratorios antivirus y antes de lanzar actualizaciones, estos programas nocivos no pueden ser detectados hasta recibir las actualizaciones por las soluciones antivirus — así mismo, usando los mecanismos heurísticos.

Los productos Dr.Web borran correctamente cualquier variante conocido de troyanos cifradores y, así mismo, permiten desinfectar hasta las modificaciones que aún no han llegado al laboratorio antivirus. Las tecnologías usadas en los productos Dr.Web dificultan considerablemente la creación por los malintencionados de las muestras muy nuevas de programas nocivos que no pueden ser detectados por los medios del núcleo antivirus Dr.Web.

El uso de Dr.Web Katana puede mejorar las posibilidades de protección de equipos que tienen instalado otro antivirus basado en firmas (no Dr.Web).

> **¡Atención!** En cualquier momento ningún programa antivirus — sin aplicar los medios de protección adicionales (tales como el sistema de restricción de acceso o control de procesos iniciados) — no pude asegurar la protección de penetración de programas nocivos aún desconocidos.

La información más detallada sobre los troyanos cifradores puede consultarse por la dirección http://antifraud.drweb.ru/encryption_trojs.

2. Peculiaridades de configuración del software antivirus para la protección contra la acción de programas cifradores

Un troyano cifrados aún desconocido al sistema de protección antivirus puede penetrar en la red local o a un equipo separado a través del spam (normalmente el mensaje contiene un adjunto o un enlace creado a propósito) usando un mensaje de messenger (que también contiene un enlace), desde un sitio web infectado o en una unidad USB infectada. La infección misma puede producirse sin que el usuario lo note — los programas nocivos de hoy se crean para que el usuario no note su funcionamiento hasta el momento necesario para los malintencionados — hasta cifrar los archivos en el equipo y/o hasta que aparezca un mensaje con una demanda del rescate.

¡Atención! La falta de atención a la protección de los datos personales entre sus amigos y socios puede causar que un mensaje con el cifrador llegue en nombre de la persona o de la empresa conocida para el destinatario— por ejemplo, de una agencia tributaria o de un banco. Además, ¡el mensaje puede ser destinado al mismo destinatario!

Si las variantes desconocidas de troyanos de la familia Trojan.Encoder penetran en el equipo, normalmente se detectan y se borran del mismo no antes de recibir la próxima actualización de los medios de protección antivirus. Por lo tanto, hay que actualizar las bases de virus lo más frecuentemente posible — no menos de una vez cada hora.

1. En caso de disponer de acceso a Internet, habilite el uso del componente Dr.Web Cloud (existe en productos **Dr.Web Security Space** (para Windows) y **Dr.Web Desktop Security Suite** (para Windows), licencia Protección integral, así como **Dr.Web Katana**. Permite encontrar los archivos nocivos más rápido, porque la información sobre los mismos se hace disponible al sistema de protección antes de recibir la actualización correspondiente.
2. Los delincuentes crean centenas y miles de nuevas muestras de programas nocivos al día, y no tiene sentido garantizar que un antivirus de archivos que busca los virus a base del conocimiento almacenado en las bases de virus, los detecte en el momento de penetración. **El módulo de protección preventiva** puede asegurar la detección de los representantes desconocidos de la familia Trojan.Encoder que usando el analizador heurístico controla los intentos de los malintencionados de realizar la acción necesaria, comparando «al vuelo» el comportamiento de programas iniciados al comportamiento de troyanos cifradores.

¡Atención! La configuración de las opciones de trabajo del Control Parental y de la Protección preventiva puede dificultar considerablemente la penetración de las muestras desconocidas de programas nocivos. Al restringir los derechos de acceso de usuarios (es decir, también de los programas iniciados), al establecer restricciones para programas de acceso a varios recursos de sistema, creamos una configuración que garantiza la integridad de nuestros datos. Incluso si el programa nocivo es desconocido para el núcleo antivirus y la protección preventiva, en estas condiciones no podrá iniciarse o se iniciará, pero será detectado en cuanto intente consultar el recurso del sistema controlado.

3. Lamentablemente, hasta el uso de la protección preventiva que permite a Dr.Web detectar hasta las variantes desconocidas de cifradores, no permite prevenir completamente el cifrado de archivos — en un equipo con Dr.Web instalado durante el análisis del proceso sospechoso el cifrador puede cifrar hasta diez archivos. Para prevenir la pérdida de datos, hay que configurar el componente «Protección contra la pérdida de datos» que forma parte de Dr.Web Security Space, así como **Dr.Web Desktop Security Suite** (para Windows), licencia Protección integral.

   ¡Atención! Como las posibilidades de respuesta a los programas cifradores de las soluciones **Dr.Web Security Space** y **Dr.Web Desktop Security Suite** (para Windows), licencia Protección integral, son iguales, todos los ejemplos de configuración pueden consultarse en Dr.Web Security Space.

Hasta si para la protección de datos ya se usa una herramienta de copia de seguridad, el uso del componente «Protección contra la pérdida de datos» también se recomienda, porque eso asegura un almacenamiento más operativo de los datos críticos para el usuario. A diferencia de programas ordinarios de copia de seguridad, Dr.Web cree y **protege** contra el acceso no sancionado de los malintencionados el almacén con las copias de archivos.

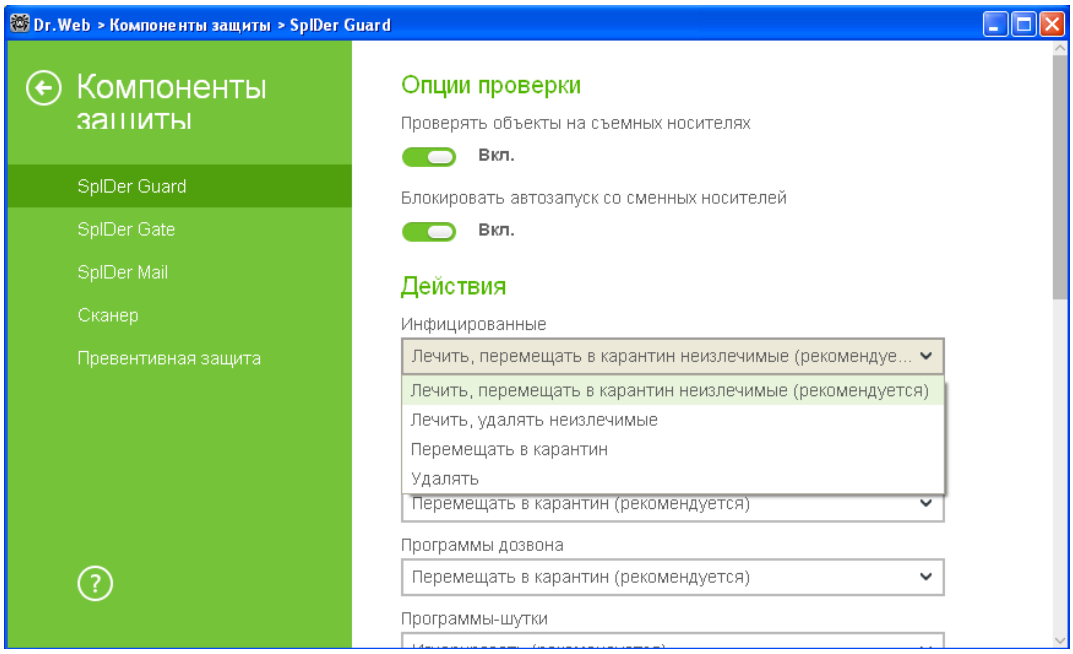
2.1. Configuración de acciones de Dr.Web Security Space con archivos nocivos

Para recuperar los datos de archivos cifrados basta con disponer del archivo nocivo mismo que realizó esta acción. Además, los archivos nocivos de la familia Trojan.Encoder son objetos que no pueden ser desinfectados. Por lo tanto, para los mismos hay que usar la acción **mover a cuarentena.**

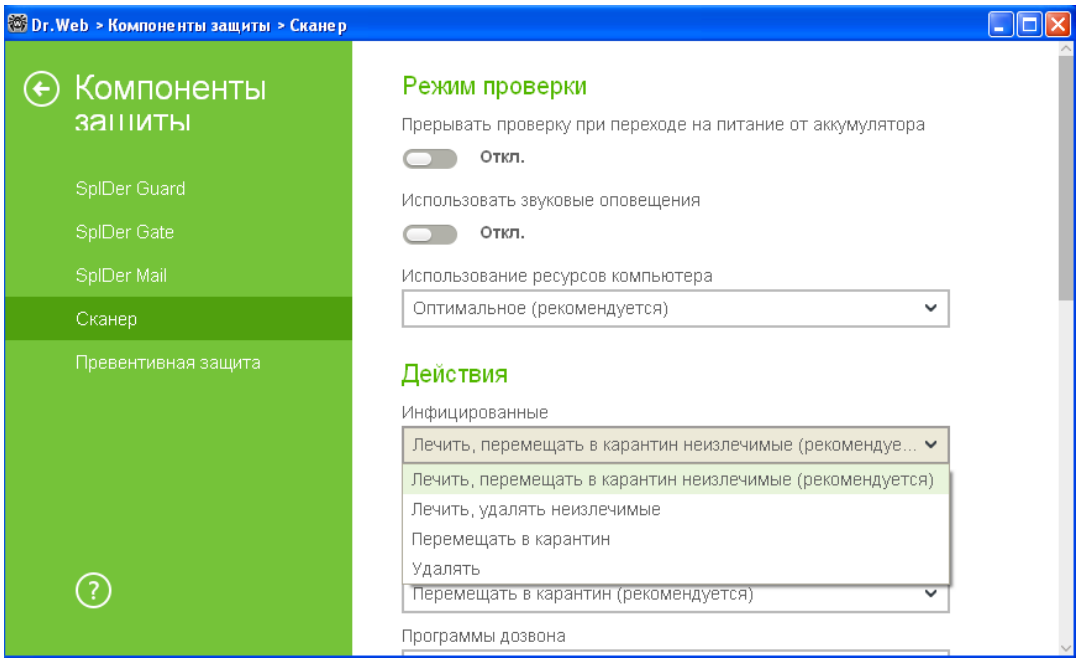
¡Atención! El inicio del escaner antivirus puede causar cambios en los datos y sus atributos del equipo. Eso, a su vez, puede impedir el análisis posterior del incidente informático o la proporción de los datos como prueba material. Se recomienda

realizar todas las acciones de recuperación de datos en la imagen del disco duro obtenido según las normas procesales.

Haga clic sobre el icono en el menú del sistema, luego en el menú que se abre pulse por orden (Modo de administrador) y el icono que aparece (Configuración). En la ventana que se abre **Configuración** seleccione el punto **Componentes de protección** y luego **SpIDer Guard**.



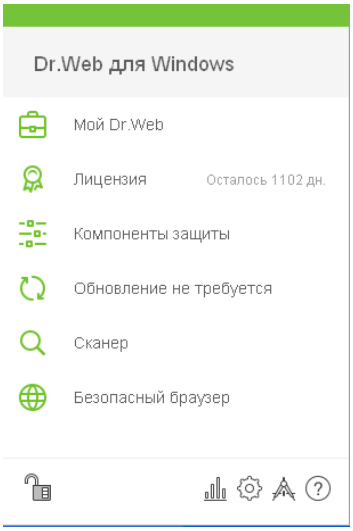
Hay que usar la misma configuración al realizar el escaneo antivirus. La configuración se realiza en la misma ventana que la configuración de SpIDer Guard, pero en la sección **Escáner**.



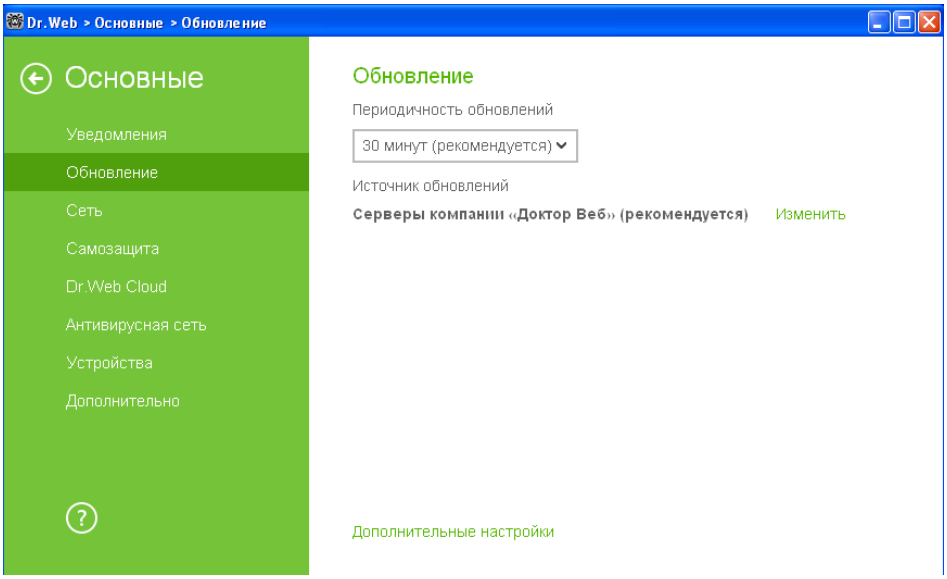
¡Atención! No borre los objetos de la cuarentena, porque en algunos casos los archivos nocivos pueden contener las claves que pueden ayudar a descifrar.

2.2. Actualización del sistema de actualizaciones Dr.Web Security Space

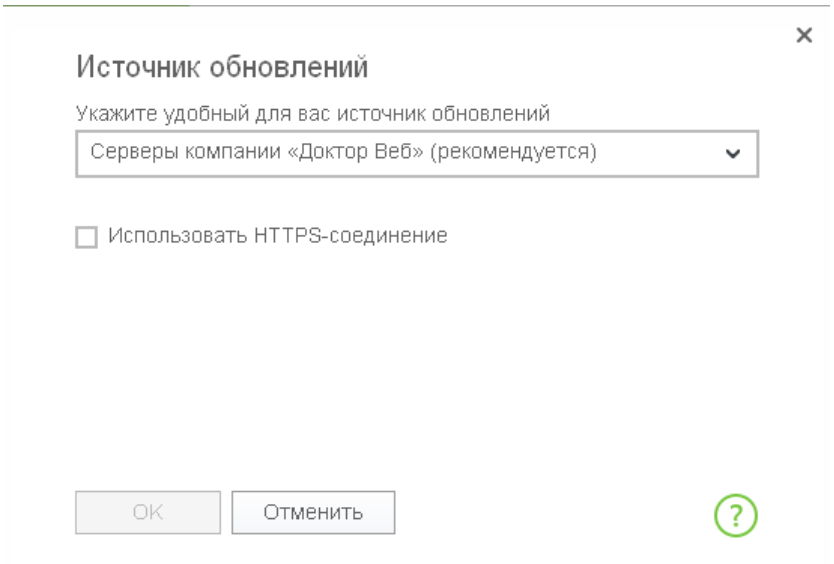
Para configurar las opciones de actualización, haya clic por orden sobre el icono en el menú del sistema, luego en el menú que se abre haga clic por orden sobre y sobre el icono que aparece .



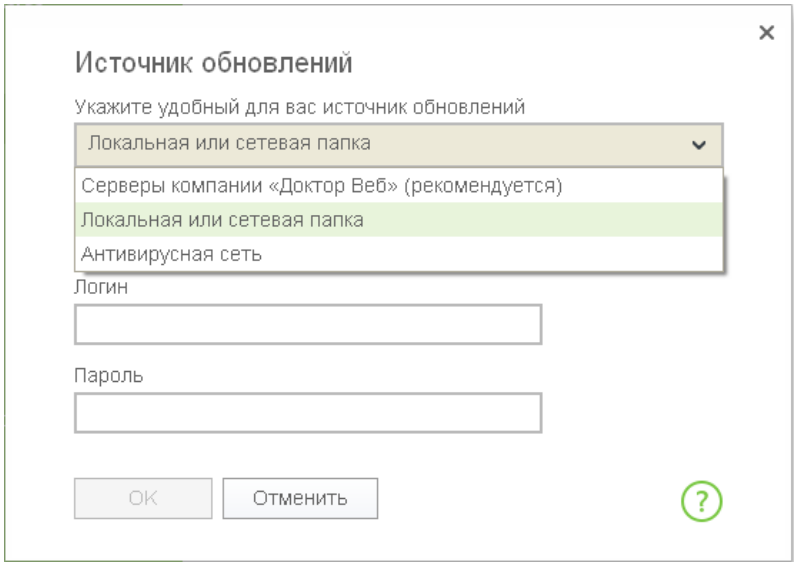
En la ventana que se abre **Configuración** seleccione **General → Actualización**.



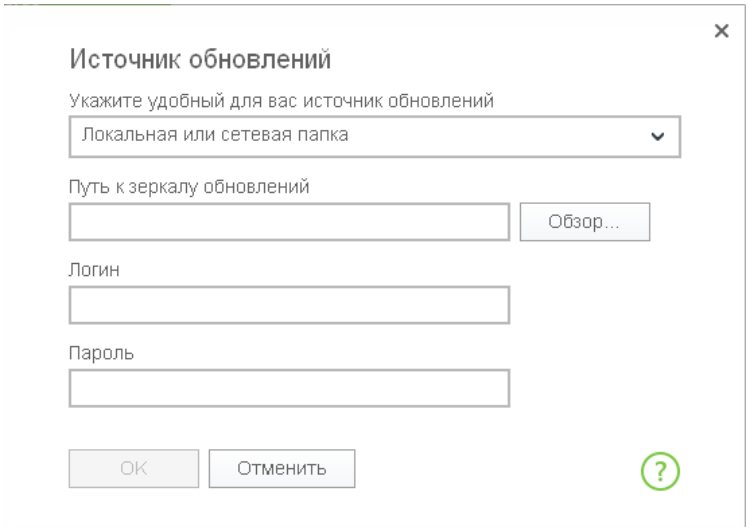
De forma predeterminada, el antivirus se actualiza desde los servidores de la empresa Doctor Web. Para cambiar el origen de actualizaciones, seleccione **Modificar**.



Hay tres opciones disponibles:

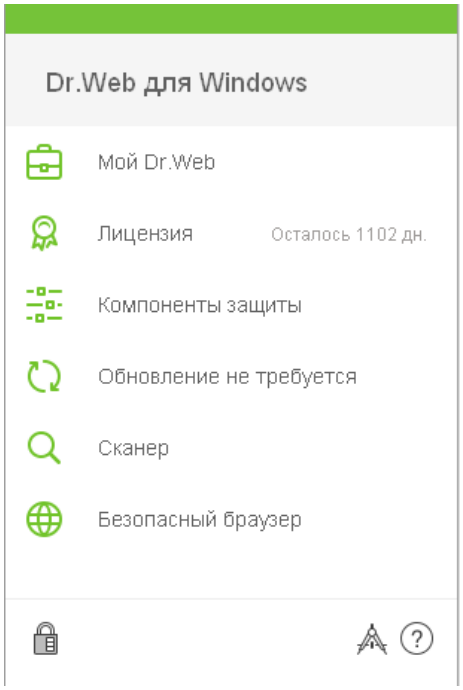


En caso de realizar una actualización de la carpeta local, indique la dirección de la carpeta y las opciones de acceso a la misma.

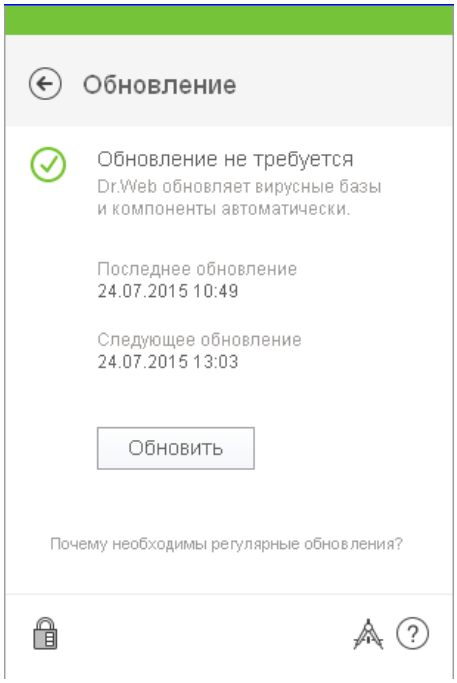


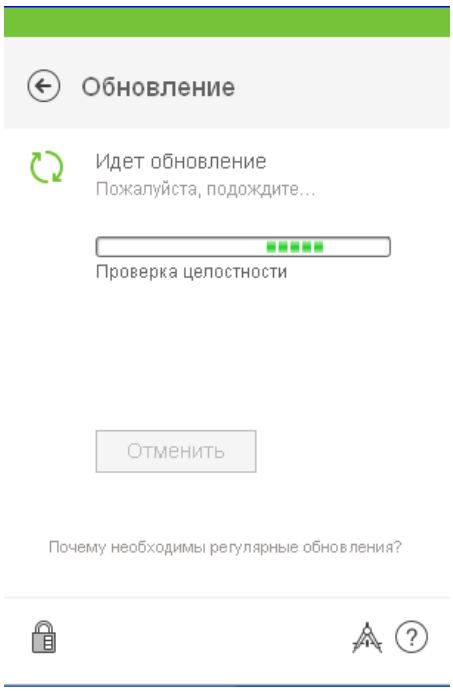
De la misma forma hay que realizar la actualización desde el servidor antivirus.

Para realizar la actualización manualmente o comprobar el estado de actualizaciones, haga clic sobre el icono en el menú del sistema y seleccione .



Para actualizar manualmente, haga clic sobre **Actualizar**.

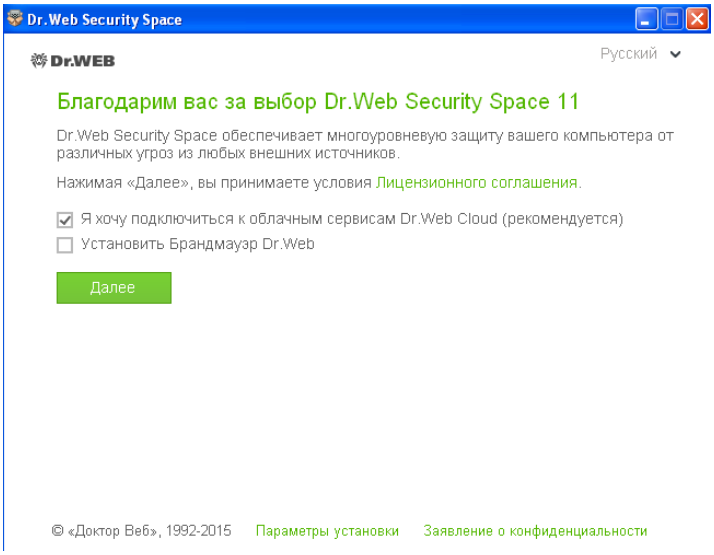




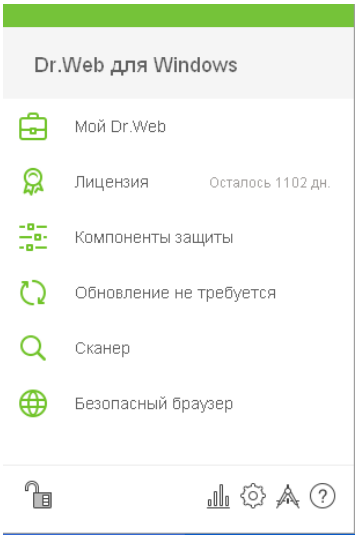
2.3. Configuración del componente Dr.Web Cloud

El uso del componente Dr.Web Cloud se ofrece ya durante la instalación del producto Dr.Web Security Space. Para el funcionamiento del componente, basta con mantener el valor predeterminado de la opción

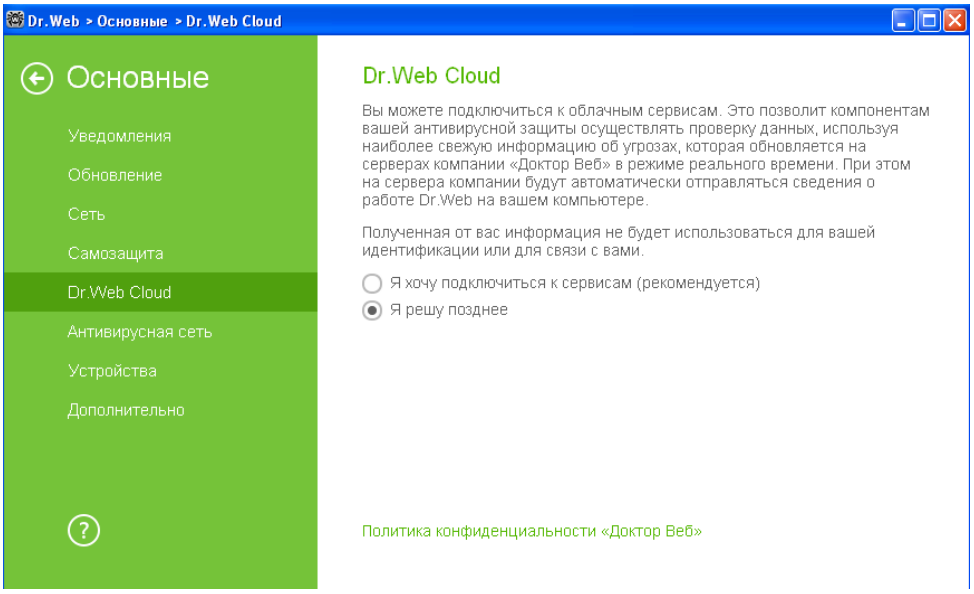
Deseo conectarme a servicios en la nube Dr.Web Cloud. Una vez finalizada la instalación, la solicitud de reputación para cada objeto analizado se realizará automáticamente y no requiere casi ningún gasto de recursos del equipo protegido.



Si durante la instalación el componente Dr.Web Cloud no estaba activado, haga clic por orden sobre los iconos y . Luego haga clic sobre el icono que aparece .



En la ventana que se abre **Configuración** seleccione el punto del menú **General → Dr.Web Cloud**.



En la ventana que se abre, seleccione **Deseo conectarme a los servicios**.

2.4. Configuración de las opciones Dr.Web Security Space que aseguran la detección de archivos nocivos anteriormente desconocidos

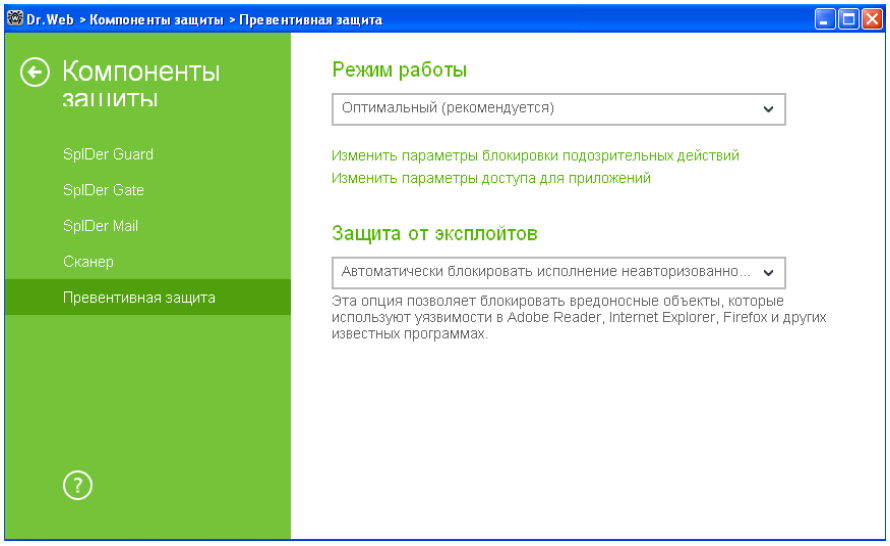
La detección de los representantes aún desconocidos de la familia Trojan.Encoder se asegura por el módulo **Protección preventiva** que controla los intentos de los programas nocivos de realizar la acción necesaria y compara «al vuelo» el comportamiento de programas iniciados con el comportamiento de los troyanos cifradores.

La detección de los programas nocivos anteriormente desconocidos se asegura por el análisis en segundo plano de procesos iniciados, así como por un análisis antivirus periódico — planificado o por demanda.

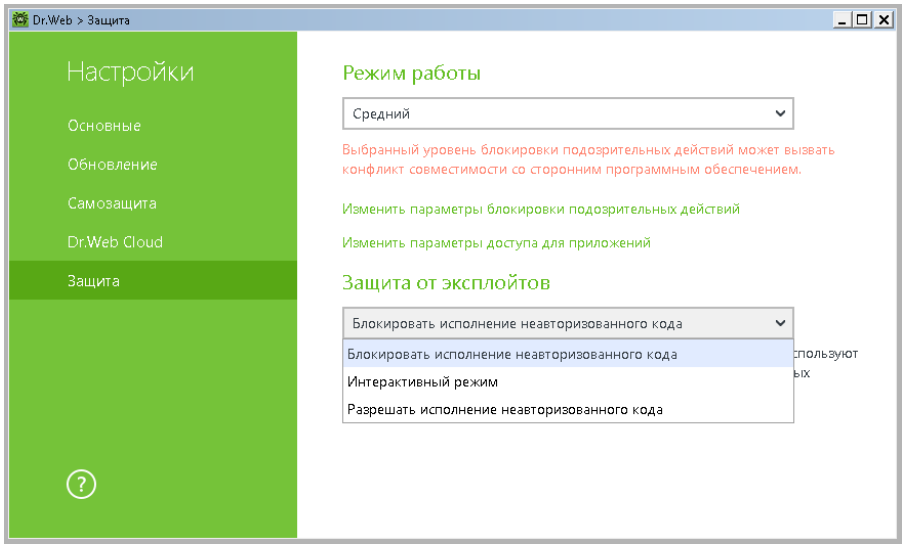
El subsistema de escaneo de segundo plano y neutralización de amenazas activas fue realizado en **Antirootkit Dr.Web**. Este subsistema constantemente está en la memoria y busca las amenazas activas en las siguientes áreas críticas de Windows: objetos de autoinicio, procesos y módulos iniciados, heurísticos de objetos de sistema, memoria operativa, MBR/VBR de unidades, BIOS de sistema del equipo. Al detectar amenazas, este subsistema puede noticiar al usuario sobre el peligro, desinfectar y bloquear el impacto peligroso.

Para configurar las opciones de protección preventiva, haga clic sobre el icono en el menú del sistema y luego en el menú que se abre por orden pulse y el icono que aparece .

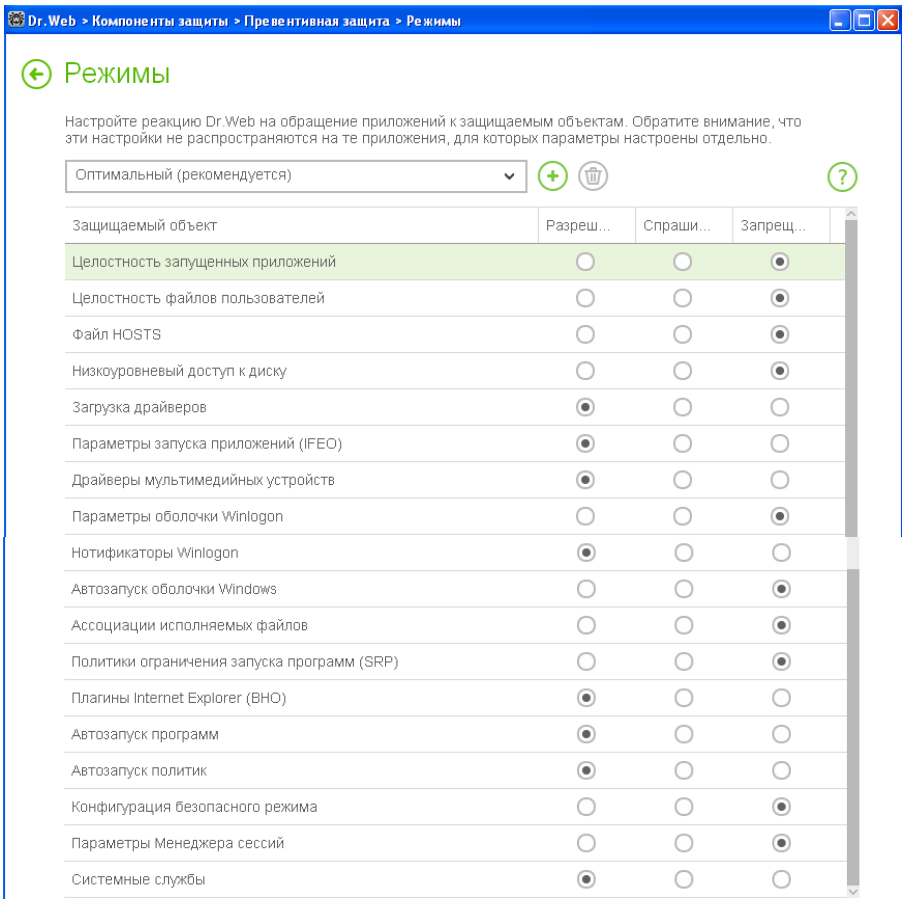
En la ventana que se abre **Configuración** seleccione el punto **Componentes de protección** y luego **Protección preventiva**.



¡Atención! En el producto Dr.Web Katana fue cambiado el nombre del componente **Protección preventiva**:



Para configurar la respuesta del antivirus a las acciones de aplicaciones terceras que pueden causar la infección de su equipo, establezca el nivel necesario de bloqueo de acciones sospechosas. La configuración de las opciones de protección preventiva permite controlar todos los intentos de modificar las áreas críticas de Windows. Para cambiar la configuración de la protección preventiva, haga clic sobre **Cambiar las opciones de bloqueo de acciones sospechosas**.



En el modo de funcionamiento **Óptimo** establecido de forma predeterminada se prohibe el cambio automático de objetos del sistema cuya modificación significa unívocamente un intento de impacti nocivo en el sistema operativo. Así mismo, se prohíbe el acceso de bajo nivel a la unidad para proteger el sistema contra la infección por bootkits y troyanos bloqueadores que infectan la entrada principal de inicio de la unidad. Para prevenir el bloqueo del acceso a actualizaciones del antivirus a través de Internet y de acceso a los sitios de fabricantes de antivirus, se prohíbe modificar el archivo HOSTS.

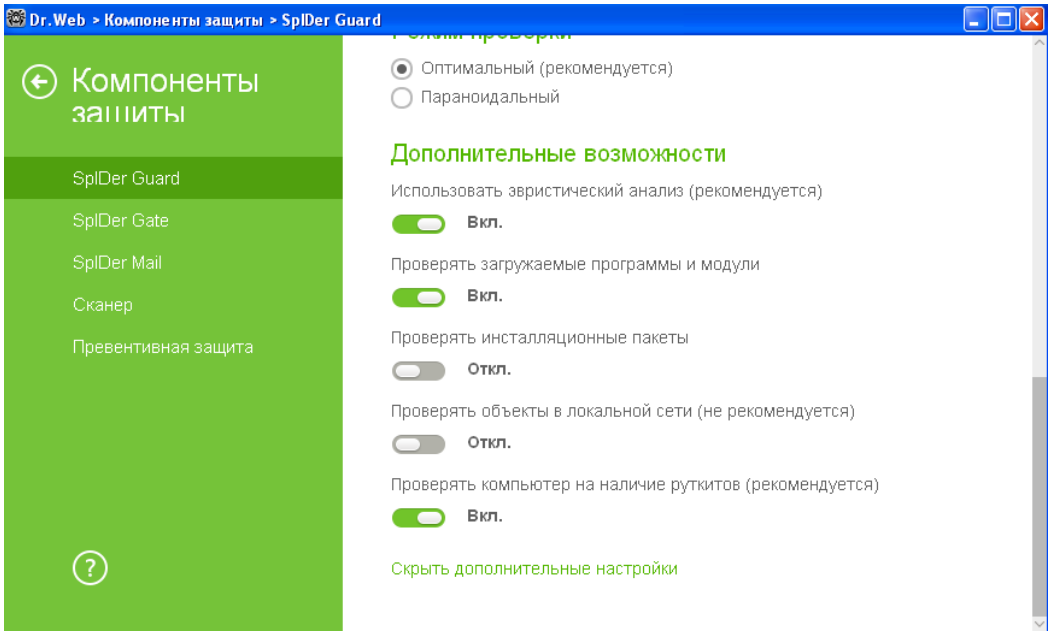
En caso de alto peligro de infección, es necesario mejorar el nivel de protección hasta **Medio**. En este modo se prohíbe adicionalmente el acceso a los objetos críticos que pueden ser potencialmente usados por los programas nocivos.

¡Atención! En este modo de protección son posibles los conflictos de compatibilidad con el software de terceros que usa los ramos del registro protegidos.

Si es necesario un control completo de acceso a los objetos críticos de Windows, se puede mejorar el nivel de protección hasta **Paranóico**. En este caso, estará disponible un control interactivo de carga de controladores y de inicio automático de programas.

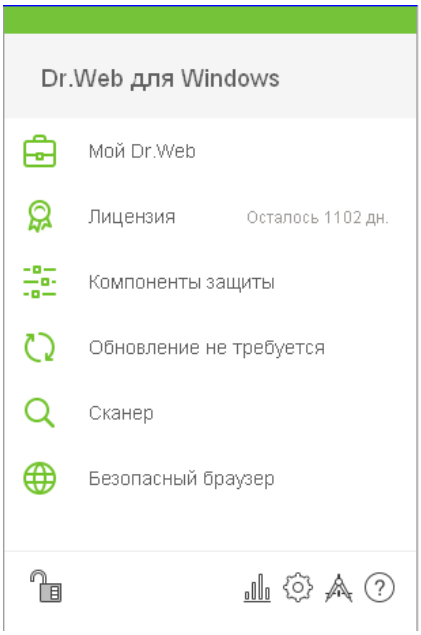
Para configurar sin ayuda las opciones de funcionamiento de la protección preventiva, establezca el nivel necesario de acceso a los objetos protegidos. El modo se cambia automáticamente por el de **Usuario.** El modo de usuario permite configurar de forma flexible la respuesta del antivirus a las acciones determinadas que pueden causar la infección de su equipo.

Para habilitar el modo de análisis en busca de rootkits, en la ventana **Configuración** seleccione **Componentes de protección → SpIDer Guard**. En la ventana que se abre haga clic sobre **Configuración avanzada**. De forma predeterminada, la función de análisis en busca de rootkits está habilitada.

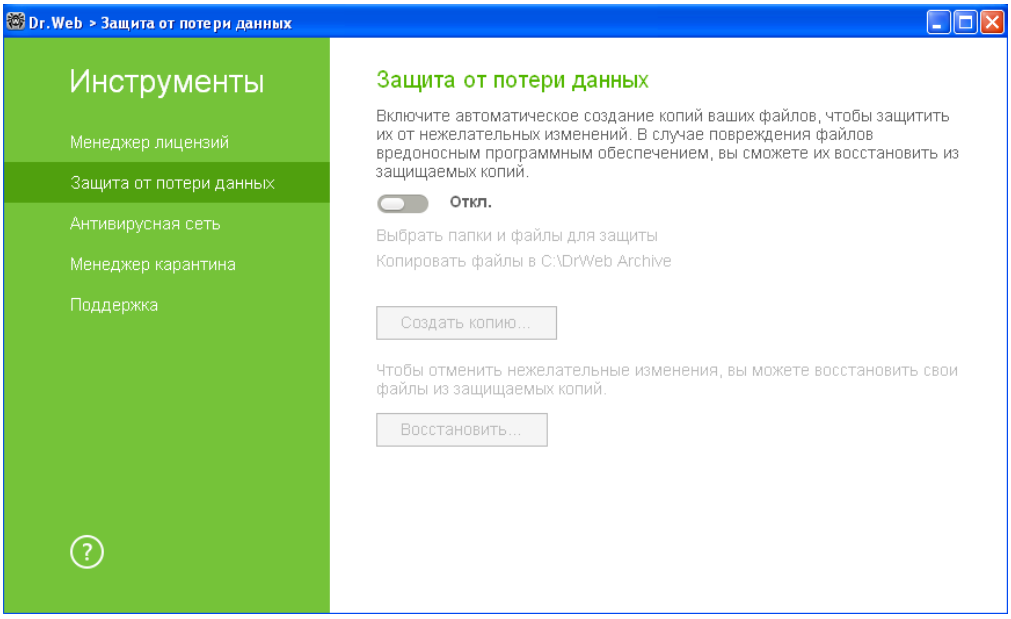


2.5. Funcionalidad «Protección contra la pérdida de datos»

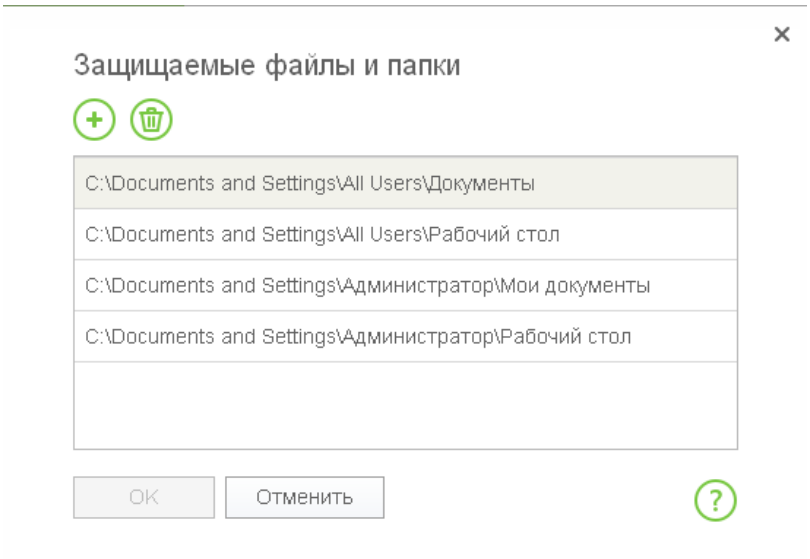
Para configurar las opciones de «Protección contra la pérdida de dato» haga clic sobre en el menú del sistema, luego en la ventana que se abre por orden haga clic sobre y el icono que aparece .



En la ventana que se abre vaya a la sección **Protección contra la pérdida de datos** y habilite la creación automática de las copias de sus datos al hacer clic sobre el interruptor.

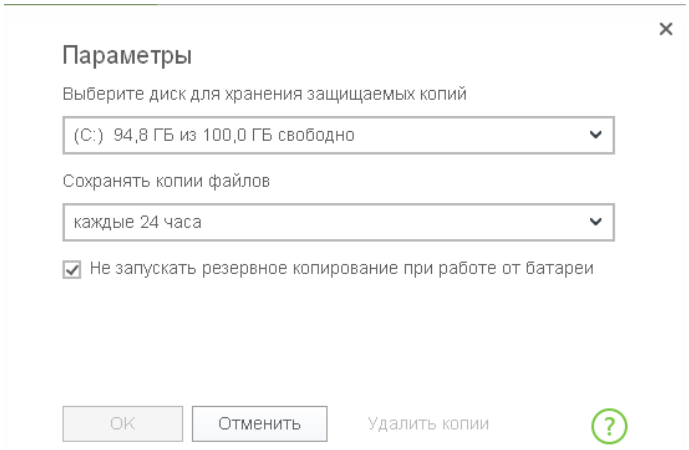


Luego hay que indicar los archivos y las carpetas que se guardarán.



Para añadir carpetas y archivos, haga clic sobre el icono ⊕ e indique los objetos necesarios para la protección.

Se puede indicar la periodicidad de creación de las copias y la ubicación para guardar las mismas al seleccionar el punto **Copiar archivos**...

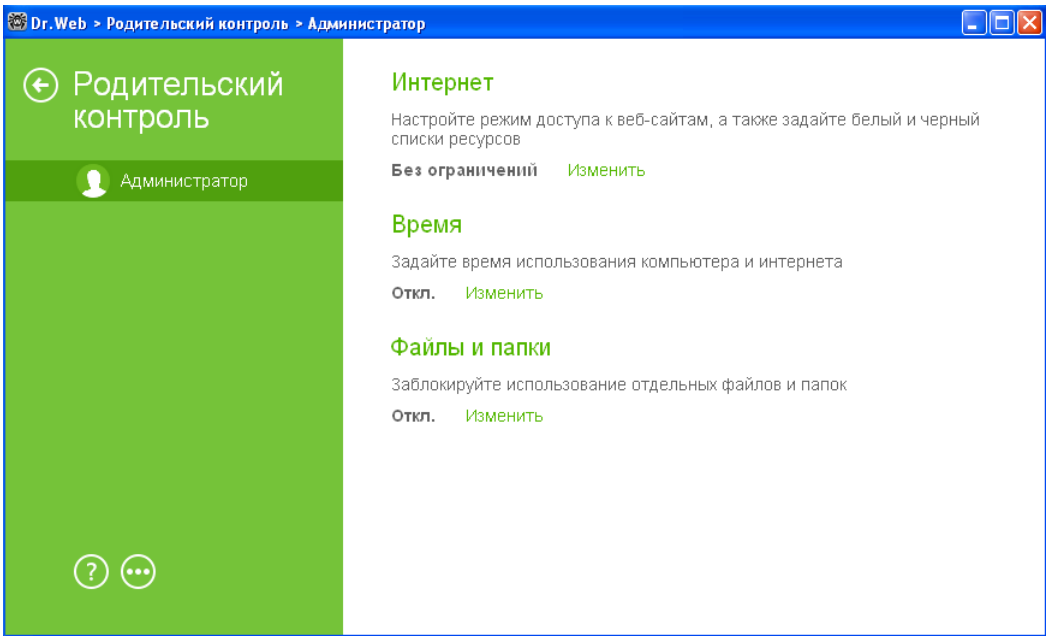


2.6. Restricción de la posibilidad de penetración de programas cifradores en el equipo

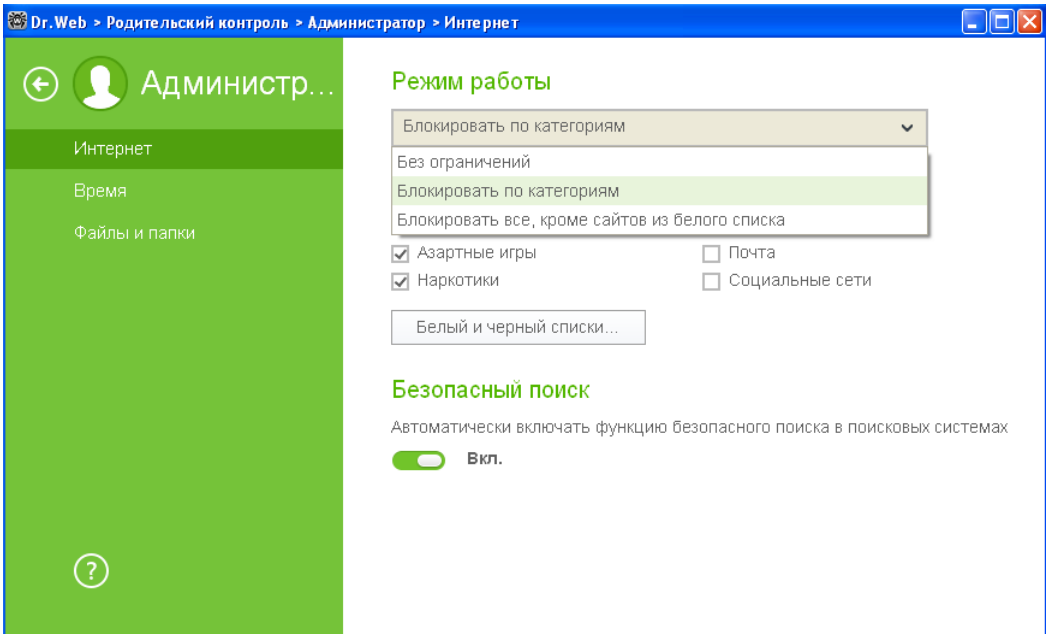
Un troyano cifrador puede penetrar en la red local o en un equipo a través de spam (normalmente el mensaje contiene un adjunto nocivo o un enlace creado a propósito), usando un mensaje de messenger (que también contiene un enlace), por medio de descargar el cifrador por el usuario mismo desde un sitio web infectado o desde una unidad USB infectada. Para menor riesgo de infección, hay que usar antispam y restringir la posibilidad de trabajo con recursos potencialmente peligrosos de la red Internet y dispositivos extraíbles.

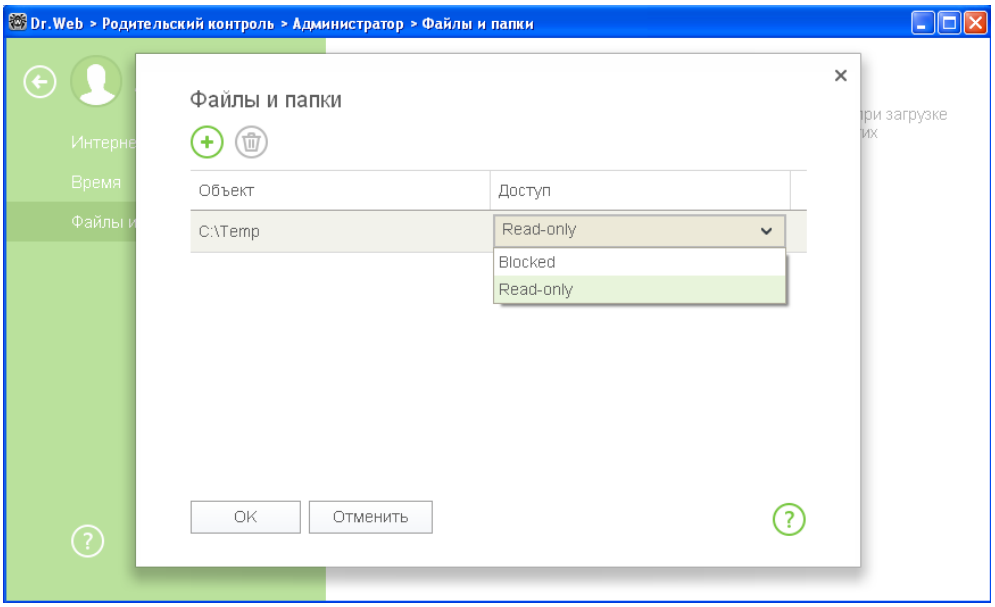
En el presente curso no se describe la configuración del antispam Dr.Web, porque el antispam empieza a funcionar de forma predeterminada desde el momento de instalación de Dr.Web Security Space y no requiere configuración adicional.

Para configurar el modo de acceso a los recursos de la red Internet, así como restringir acceso a archivos y carpetas, por orden haga clic sobre los iconos y . Luego haga clic sobre el icono que aparece y en la ventana **Configuración** vaya al punto del menú **Control parental**.



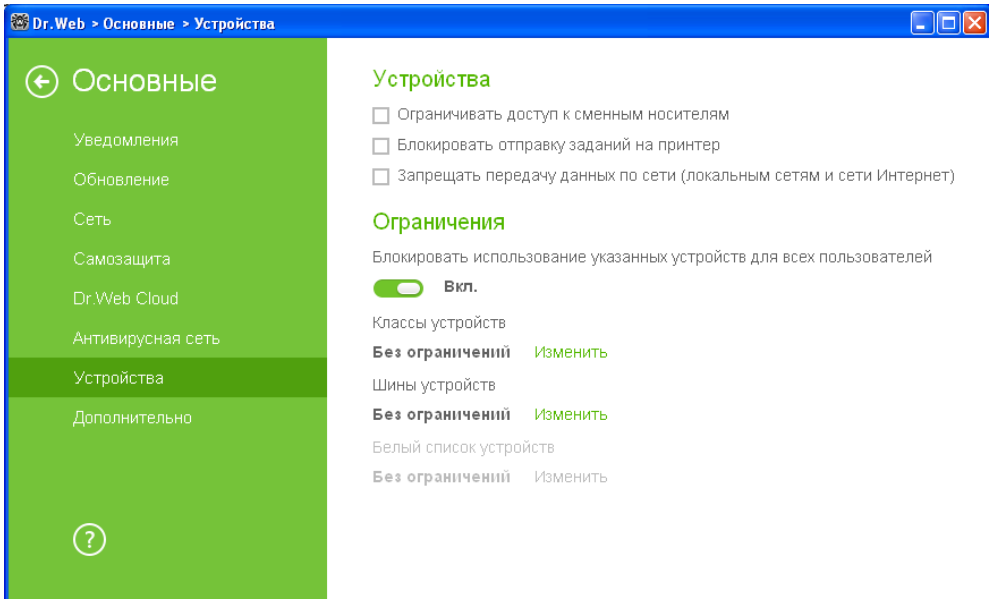
En la ventana que se abre seleccione el usuario para el cual hay que configurar las restricciones y realizar la configuración necesaria.



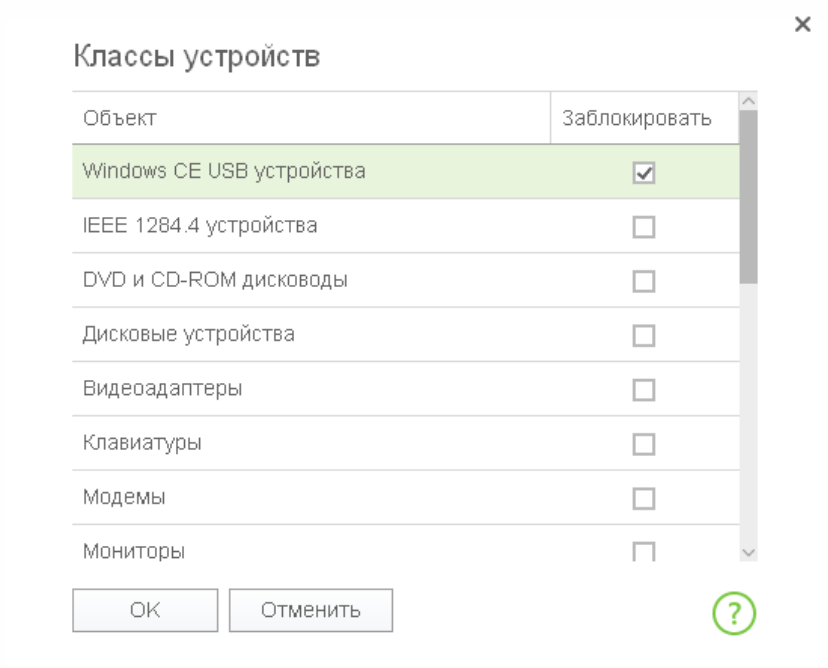


De forma predeterminada, las restricciones están deshabilitadas

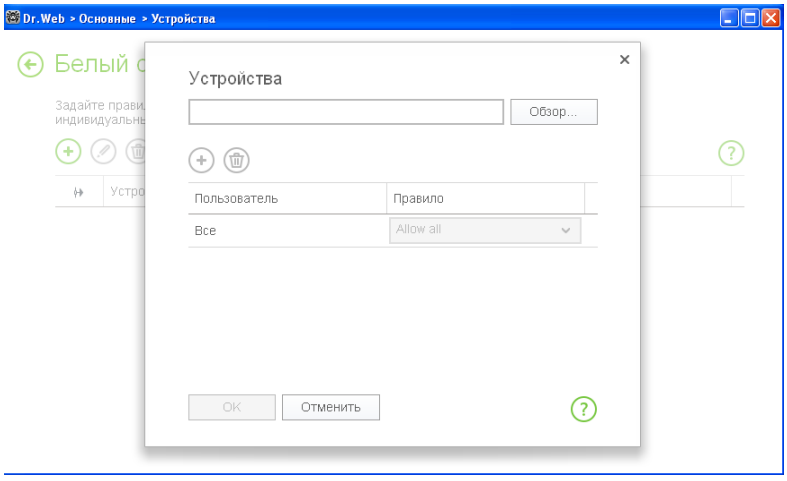
Para configurar las restricciones de unidades extraíbles, en la ventana **Configuración** seleccione **General → Dispositivos**.



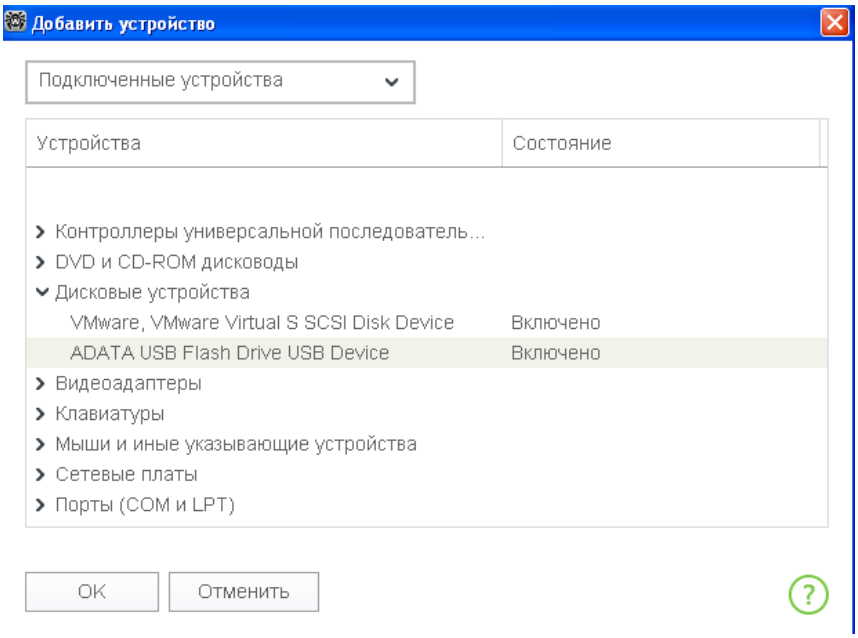
En esta ventana seleccione **Restringir acceso a dispositivos extraíbles**. Luego haga clic sobre **Modificar** para las clases de dispositivos y seleccione las clases de dispositivos necesarias.



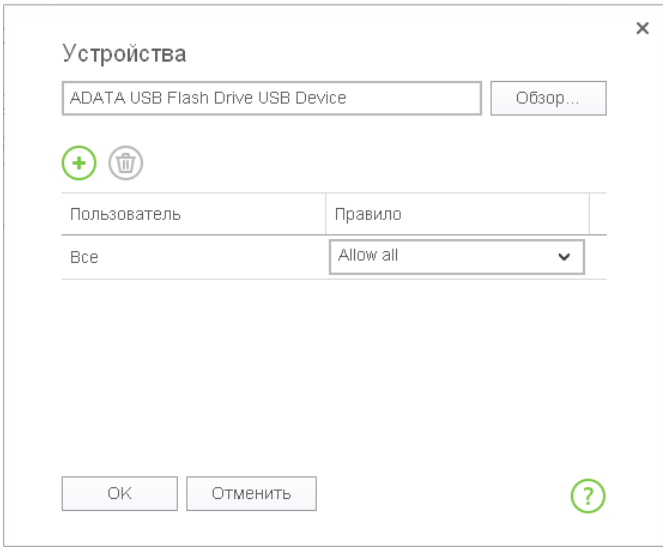
Luego aparecerá la posibilidad de configuración para la sección **Lista blanca de dispositivos**. Si es necesario usar solo los dispositivos extraíbles permitidos, haga clic sobre **Modificar** → .



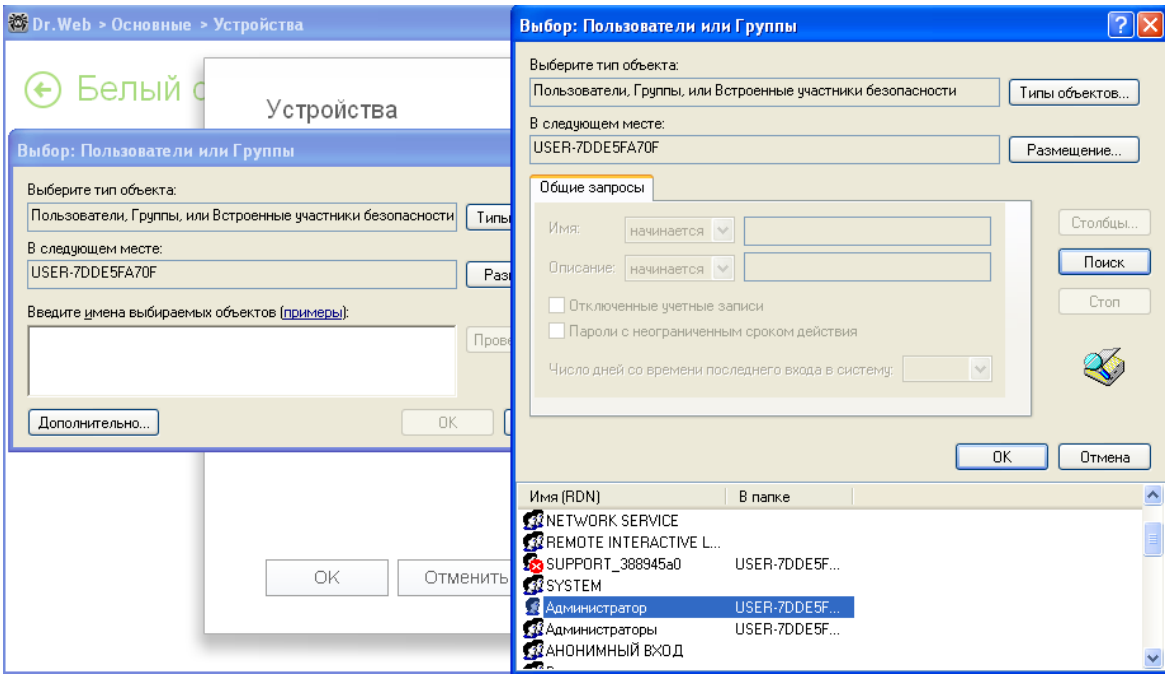
En la ventana que se abre haga clic sobre **Examinar** y seleccione el dispositivo necesario.



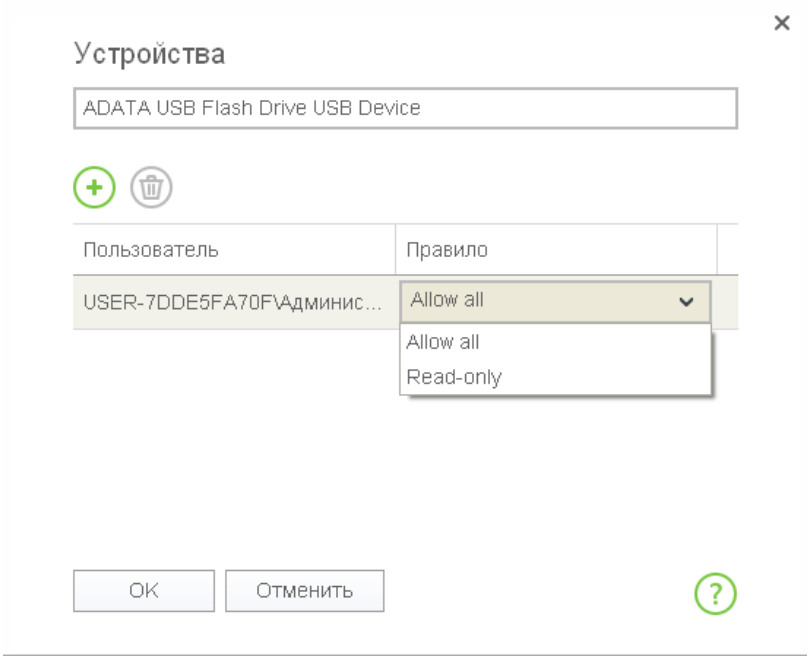
Confirme la selección al hacer clic sobre **Aceptar**.



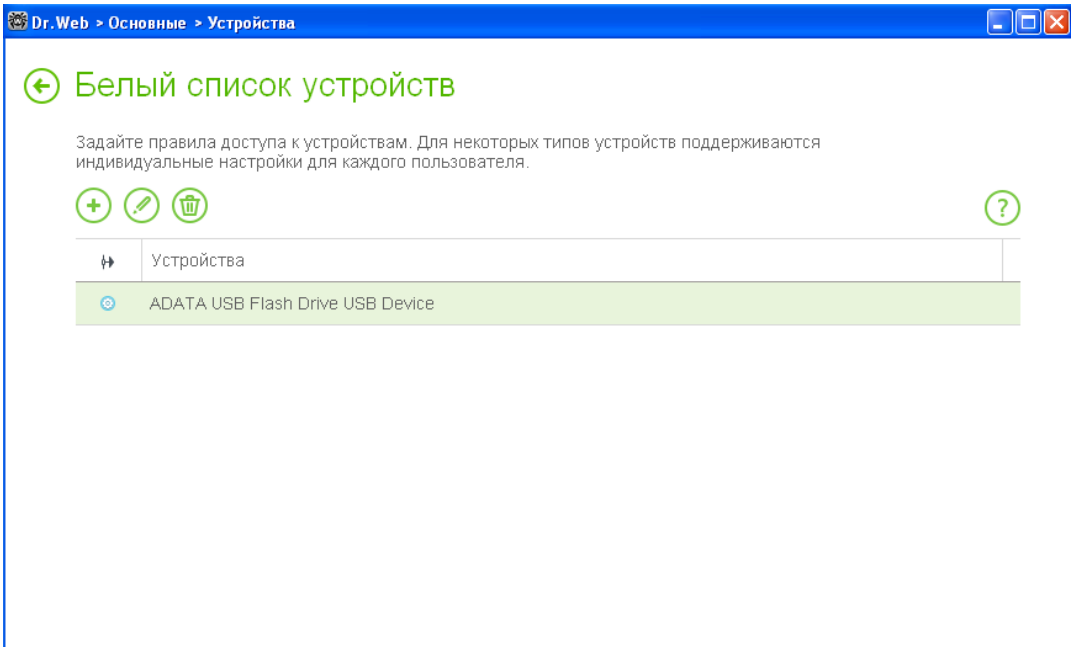
Si es necesario permitir el uso de este dispositivo solo para los usuarios determinados del equipo, haga clic sobre ⊕ y seleccione el usuario necesario.



Indique los derechos de uso de este dispositivo.



Confirme la selección.



3. Recomendaciones de la empresa Doctor Web sobre la protección del equipo contra los programas cifradores

Según las estadísticas, en más de 90% de los casos, las víctimas mismas inician los cifradores

- No hay que aceptar las propuestas de la red Internet de iniciar un adjunto o abrir un documento (normalmente son archivos creados a propósito por los malintencionados en formatos doc y pdf, que también frecuentemente se colocan en los archivos archivados con formatos.**zip**, .**rar**, .**7z** y .**cab**., porque el escaneo de archivos archivados frecuentemente se deshabilita para mayor rendimiento).
- Use las soluciones que tienen funcionalidad de copias de seguridad (creación de copias de archivos o de todo el sistema). Nunca se recomienda crear las copias de seguridad por medio de copiar los archivos manualmente, ni guardar las copias de seguridad en el equipo mismo. No se recomienda guardar las copias de seguridad en otro disco duro ni en una carpeta de red que puede ser consultada desde un equipo local. Se recomienda usar los dispositivos extraíbles y/o los almacenes de la nube, así como crear o guardar las copias de seguridad cifradas. De esta forma, los archivos serán protegidos no solo contra los programas cifradores, sino también contra los fallos de los equipos informáticos.

¡Atención! Antes de crear la copia de seguridad, hay que asegurarse de que los archivos copiados ya no están cifrados y no sustituyen las versiones de archivos no cifradas.

A partir del SO Windows Vista, los sistemas operativos Windows contienen un servicio de protección del sistema en todas las unidades que crea las copias de seguridad de archivos y carpetas durante el archivado o la creación del punto de recuperación del sistema. De forma predeterminada, este servicio está activado solo para la sección del sistema.

¡Atención! El uso de este servicio no protege contra las acciones de programas cifradores, porque los mismos pueden desactivar este servicio y destruir las copias anteriormente creadas.

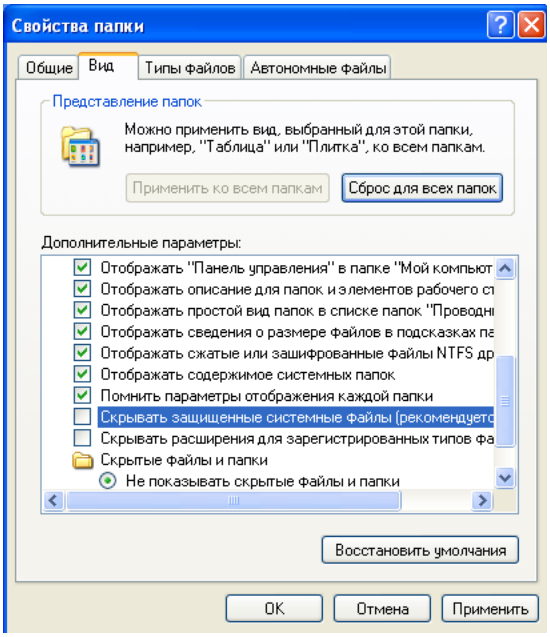
- No abra los adjuntos de correo de remitentes desconocidos. En la mayoría de los casos, los programas cifradores se difunden a través de los adjuntos de correo. La tarea del malintencionado es asegurar al usuario para que abra el adjunto del mensaje o siga el enlace.
- Si sus datos fueron cifrados, no hay que usar sin consultar a los especialistas los programas para descifrar los datos, cambiar las extensiones de los archivos cifrados, etc. Como resultado de estas acciones, Vd. puede perder de forma irrecuperable sus datos — no podrán ser localizados y recuperados ni siquiera por una utilidad especial para descifrar.
- Active la visualización de las extensiones de archivos (véase más abajo, p.3.1). Por la ausencia de visualización de extensiones las víctimas no ven qué hay en realidad dentro de archivos.
- Use solo los programas de licencia.
- Instale de forma oportuna las actualizaciones de seguridad del sistema operativo y de todos los programas instalados en su equipo.
- Configure los derechos de acceso para todos los usuarios que trabajan en el equipo, a los datos y carpetas de red usadas. En caso contrario, la infección del equipo puede causar el cifrado de todos los documentos para todos los usuarios — así mismo, en todas las carpetas de red.

Par la información más detallada en caso de infección por un cifrador, consulte las direcciones http://legal.drweb.ru/encoder.

3.1. Habilitar la visualización de extensiones de nombres de archivos

Para habilitar la visualización de las extensiones de archivos:

- Para **Windows XP:** en el menú **Inicio** seleccione **Configuración → Panel de control → Propiedades de carpetas** y desactive la casilla para la opción **Ocultar extensiones para los tipos de archivos registrados**.



- para **Windows 7**: en el teclado, pulse Alt izquierdo. En el menú que aparece pulse **Servicio → Opciones de carpetas,** en la ventana que se abre vaya a la pestaña **Vista** y en el listado de opciones adicionales desactive la casilla para la opción **Ocultar extensiones para los tipos de archivos registrados**.
- para **Windows 8/8.1:** abra cualquier carpeta o inicie el Explorador de Windows 8, al pulsar las teclas Windows + E. En el menú principal del explorador vaya a la carpeta **Ver** y active la casilla cerca de la línea **Extensiones de nombres de archivos** — si la misma está activada, se las extensiones se visualizan (no solo en la carpeta seleccionada, sino también en todos los sitios del equipo), si no — las extensiones están ocultas.

4. Acciones del usuario en caso de detectar los archivos cifrados y/o demandar un rescate

Para mejorar las posibilidades de recuperación correcta de los datos cifrados, en ningún caso se puede:

- Cambiar la extensión de los archivos cifrados;
- Reinstalar el sistema;
- Usar sin ayuda — sin recomendaciones de especialistas del soporte técnico de la empresa Doctor Web— cualquier programa para descifrar /recuperar los datos;
- borrar/cambiar nombre de algún archivo o programa (entre ellos, los temporales);
- en caso de haber iniciado el escaneo antivirus — no se puede realizar ninguna acción irrecuperable para desinfectar/borrar los objetos nocivos.

4.1. Utilidades para descifrar

Se puede descifrar los archivos cifrados por los malintencionados usando las utilidades especiales proporcionadas por el servicio de soporte técnico de la empresa Doctor Web por solicitud. Lamentablemente, el número de tipos de troyanos que aparecen todos los días no permite crear las utilidades para todos ellos. Por eso, si sus archivos fueron cifrados por un troyano aún desconocido — se puede solicitar un servicio de descifrar (https://support.drweb.ru/new/free_unlocker/?keyno=&for_decode=1). Para los usuarios comerciales de Dr.Web este servicio es gratuito.

Si Vd. necesita un servicio de descifrar, envíe para analizar no menos de 3-5 archivos cifrados de varios tipos. Además, la información adicional puede ayudar a descifrar — la descripción del proceso de infección, un mensaje con la demanda del rescate etc. Si se conoce el archivo al iniciar el cual los malintencionados han podido cifrar sus archivos — se recomienda adjuntarlo también a la solicitud.

¡Atención! Antes de iniciar las utilidades, cree las copias de archivos cifrados.

4.2. Dónde pueden ubicarse los archivos de programas cifradores

En caso de haber detectado un archivo sospechoso cuyo inicio pudo causar la infección del equipo y el cifrado de archivos — envíe el archivo sospechoso para analizar. Los archivos pueden ser localizados siguiendo estas rutas:

APPDATA	SO Windows NT/2000/XP: Unidad:\Documents and Settings\%UserName%\Application Data\ %USERPROFILE%\Local Settings\Application Data SO Windows Vista/7/8: Unidad:\Users\%UserName%\AppData\Roaming\ %USERPROFILE%\AppData\Local
TEMP (catálogo temporal)	%TEMP%*.tmp %TEMP%*.tmp* %TEMP%* %WINDIR%\Temp
Catálogo temporal de Internet Explorer	SO Windows NT/2000/XP: %USERPROFILE%\Local Settings\Temporary Internet Files\ SO Windows Vista/7/8: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\ ..\temporary internet files\content.ie5\ ..\temporary internet files\content.ie5*\
Escritorio	%UserProfile%\Desktop\
Papelera de reciclaje	Unidad:\Recycler\ Unidad:\$Recycle.Bin\ Unidad:\$Recycle.Bin\s-1-5-21-??????????-??????????-??????????-1000 (? -- 0-9)
Catálogo de sistema	%WinDir% %SystemRoot%\system32
Catálogo de documentos del usuario	%USERPROFILE%\Mis documentos\ %USERPROFILE%\Mis documentos\Downloads
Catálogo para descargar archivos en explorador web	%USERPROFILE%\Downloads
Catálogo de autoinicio	%USERPROFILE%\Menú principal\Programas\Autoinicio

¡Atención! Los archivos Trojan.Encoder pueden ubicarse no solo en los sitios indicados más arriba.