

# Настрой-ка Dr.Web от шифровальщиков!

Рекомендации для максимального снижения риска  
заражения троянцем-вымогателем



**Троянцы-шифровальщики (семейство Trojan.Encoder)** — вредоносные программы, которые отыскивают на дисках инфицированного компьютера или в памяти мобильного устройства пользовательские файлы, после чего шифруют их и требуют у жертвы выкуп за расшифровку.

Все шифровальщики относятся к вредоносным файлам (троянцам), которые самостоятельно распространяться и запускаться не могут. По статистике «Доктор Веб»:

| более чем в 90% случаев                                                  | только в 10% случаев  |
|--------------------------------------------------------------------------|-----------------------|
| пользователи собственными руками запускают на компьютере шифровальщиков. | расшифровка возможна. |

## Это нужно знать

Криминальные группировки, занимающиеся разработкой вредоносных программ, тестируют их **на необнаружение** всеми актуальными антивирусными решениями. В результате в «дикую природу» выпускаются только те вредоносные программы, которые гарантированно не обнаруживаются (до получения обновлений) антивирусами.

Шифровальщик может попасть даже на защищенный (любым) антивирусом компьютер — если троянец еще не известен вирусной базе или если антивирус не содержит технологий превентивной защиты. Ни один антивирус не распознает все вредоносные программы в любой момент времени.

**А это значит, что никто не застрахован от заражения новым, неизвестным шифровальщиком — если вы не настроили свою систему защиты.**

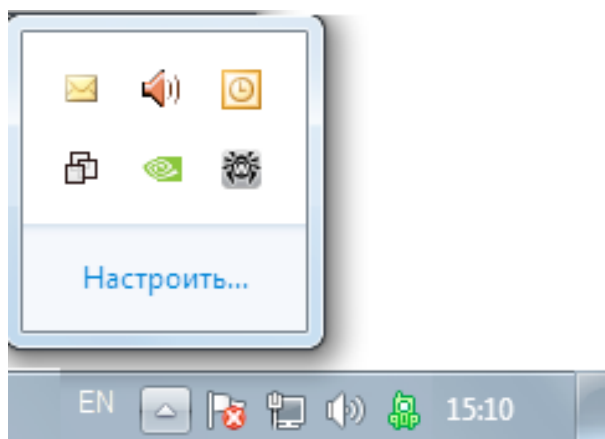
# Настрой-ка Dr.Web

Элементарные правила настройки Dr.Web помогают не допустить заражения шифровальщиком — даже неизвестным антивирусному ядру.

## Dr.Web должен быть всегда включен

А если компьютер подключен к сети Интернет или к нему подсоединен внешний носитель информации, не проверенный до подключения на вирусы, — отключать в это время Dr.Web категорически нельзя.

**О том, что Dr.Web включен, а значит, защищает ваш ПК, должен свидетельствовать вот такой значок агента Dr.Web в системном трее.**



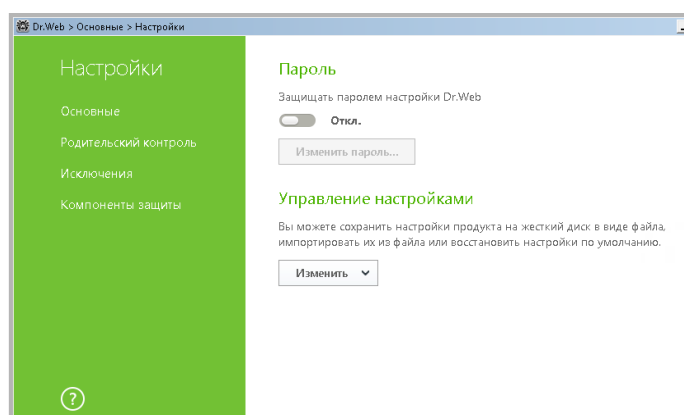
Отсутствие значка агента, значок с восклицательным знаком или крестиком означает, что Dr.Web выключен и компьютер остался без антивирусной защиты. В этом случае немедленно выполните перезагрузку компьютера. Если проблема останется — срочно [обратитесь в службу поддержки «Доктор Веб»](#).

## А ваш Dr.Web сейчас включен?

## Пароль к Dr.Web должен быть установлен

Установка пароля гарантирует невозможность отключения защиты Dr.Web — в том числе в случае взлома.

Чтобы установить пароль доступа к Dr.Web



Нажмите на значок  (значок изменит вид на ) и, нажав на появившийся значок , выберите в меню **Настройки** пункт **Основные**. Нажмите на переключатель и далее на кнопку **Изменить пароль**.

**Внимание!** Не рекомендуется устанавливать пароль, совпадающий с паролем доступа к компьютеру или устройству. Пароль к Dr.Web нельзя хранить на этом же компьютере.

## А в вашем Dr.Web пароль установлен?

**Все компоненты защиты Dr.Web должны быть всегда включены**

Каждый компонент Dr.Web Security Space участвует в защите от троянцев-вымогателей.

Отключение — пусть только одного из них и даже временно — означает неизбежное понижение защиты.

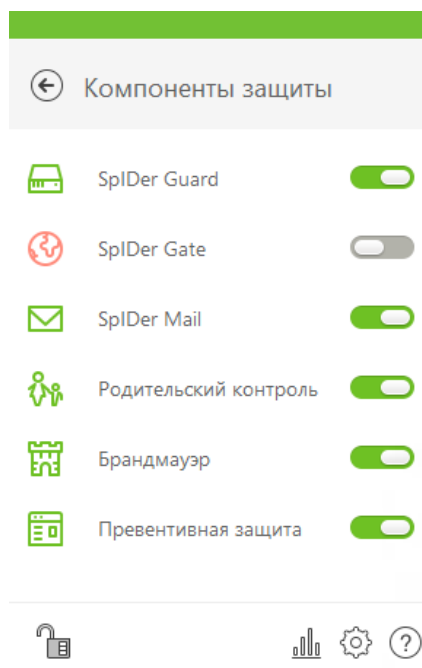
- **Dr.Web SpIDer Guard** обнаружит вредоносные программы в момент их запуска — даже если вредоносные компоненты были получены в зашифрованном виде и не были обнаружены в момент загрузки.

- Шифровальщик может проникнуть на компьютер в том числе и через сообщение электронной почты. Как правило, такое письмо содержит вредоносное вложение или специально сформированную ссылку.  
**Антивспам** Dr.Web отсеивает письма с вредоносным содержанием по признакам, характерным для писем злоумышленников — даже если антивирусное ядро еще не получило обновление, содержащее сведения о новейшей угрозе. Антивспам Dr.Web не нужно обучать — он сам знает, как действовать!
- **Dr.Web SpIDer Gate и Родительский контроль** не дадут вам перейти на опасный сайт, если ссылка на скачивание троянца придет в письме. Входящий в состав Dr.Web Security Space сервис сканирования почтового и веб-трафика построен на уникальных алгоритмах, обеспечивающих высочайшую скорость проверки и качество обнаружения вредоносных программ.
- **Брандмауэр Dr.Web** позволяет настроить ограничения для программ, имеющих доступ в сеть Интернет.

И это не все компоненты Dr.Web, обеспечивающие обнаружение вирусов и троянцев!

## Чтобы узнать, есть ли в вашем Dr.Web отключенные компоненты

Посмотрите в системный трей: если в вашем Dr.Web есть отключенные компоненты, значок Dr.Web будет выглядеть так: 🚫



## Чтобы увидеть, какие компоненты отключены

Кликните на значок агента Dr.Web и далее на пункт **Компоненты защиты** — откроется меню агента Dr.Web.

## А в вашем Dr.Web все компоненты включены?

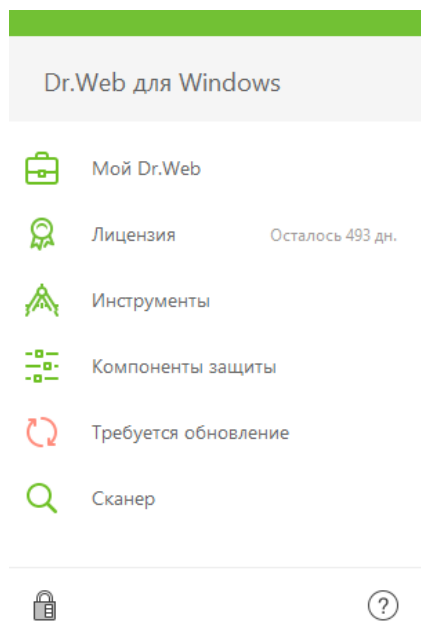
## Обновлять антивирус нужно часто

### Обновлять антивирус нужно сразу после поступления обновлений.

Для этого достаточно не отключать настройки обновлений, заданные разработчиком Dr.Web, — антивирус будет обновляться самостоятельно и вовремя.

Но еще очень важно ПРОВОДИТЬ ПЕРЕЗАГРУЗКУ ПК после обновлений, требующих такой перезагрузки, — как бы часто Dr.Web ни просил вас это делать. Потому что только после перезагрузки устанавливаются новые драйверы перехвата ранее неизвестных вредоносных программ, а также исправления для потенциальных уязвимостей защиты Dr.Web.

**Внимание!** Всего за одни сутки на анализ в антивирусную лабораторию «Доктор Веб» поступает до миллиона новых потенциально вредоносных файлов. Необновление Dr.Web даже в течение нескольких часов — это возможность пропуска сотен ранее неизвестных (в том числе для эвристического анализатора Dr.Web) вредоносных файлов. А между тем всего одному троянцу-банкеру достаточно от 1 до 3 минут, чтобы похитить деньги со счета пользователя.



### Чтобы проверить дату и актуальность обновлений

Кликните на значок  в системном трее. Статус обновлений будет показан в открывшемся меню.

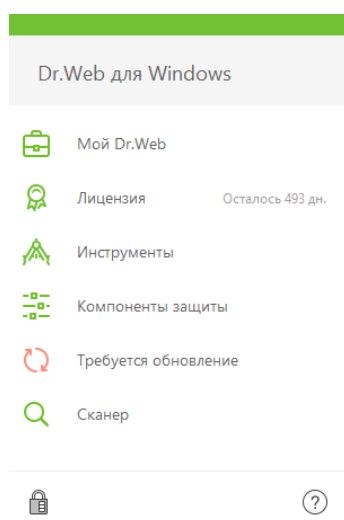
## А когда последнее обновление было в вашем Dr.Web?

## Исключения из проверки могут использоваться только в экстренных случаях

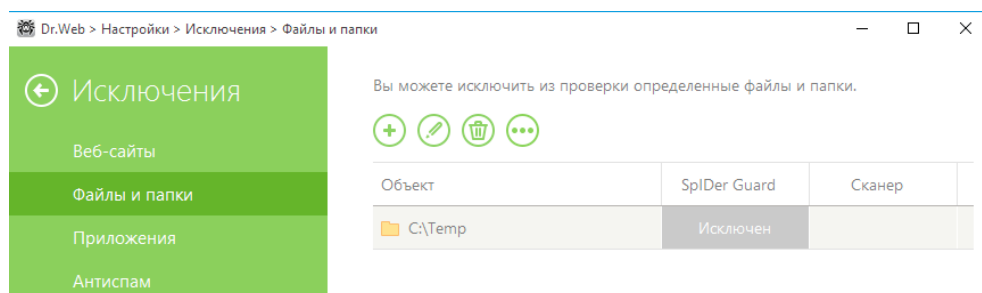
**Исключения из проверки могут ускорить сканирование, но чаще всего за счет понижения уровня безопасности.** Вирусописатели знают, ЧТО пользователи любят исключать из проверки, и активно это используют в своих преступных целях.

Наши программы максимально оптимизированы и бережно относятся к ресурсам компьютера. Мы не рекомендуем самостоятельно что-либо исключать из проверки Dr.Web, потому что не каждый пользователь имеет достаточно знаний, чтобы оценить риски такой настройки. Исключения — это способ обхода каких-либо проблемных ситуаций. Как сделать это правильно, могут порекомендовать только в техподдержке «Доктор Веб».

**Чтобы проверить, используются ли в вашем Dr.Web исключения из проверки, понижающие уровень защиты**



Кликните на значок  в системном трее. В появившемся меню кликните на значок  (значок изменит вид на ) и, нажав на появившийся значок , выберите **Настройки → Исключения**.



**Внимание!** Если в исключениях заданы маски типа \*.exe или \*.dll, Dr.Web не будет проверять все объекты, подходящие под такую маску, — т. е. все исполняемые файлы и программные библиотеки!

**Внимание!** Не рекомендуется исключать проверку трафика для используемых программ — это приведет к тому, что никакое вредоносное ПО, загруженное данными программами, проверяться не будет.

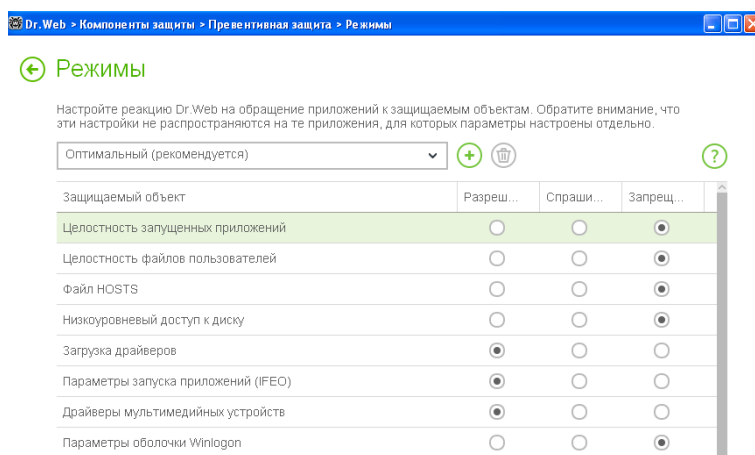
## А в вашем Dr.Web установлены какие-либо исключения из проверки?

## Превентивная защита должна быть включена

**Сегодня Превентивная защита — один из самых важных компонентов в системе комплексной защиты Dr.Web.**

По схожести поведения подозрительной (пока неизвестной Dr.Web) программы с известными моделями поведения уже известных вредоносных программ Превентивная защита Dr.Web умеет распознавать и блокировать такие программы благодаря целому набору разнообразных **технологий**, действующих на опережение и не зависящих от наличия сигнатур для них в вирусной базе Dr.Web.

**Не рекомендуется отключать превентивную защиту** — ее работа существенно затрудняет возможность украсть ваши данные и деньги для троянцев-шифровальщиков, блокировщиков, банковских троянцев и иных видов наиболее опасных вредоносных программ.



**Внимание!** Для дополнительной защиты от шифровальщиков в настройках компонента Превентивная защита всегда должно быть установлено «Запрещать» для пунктов «Целостность запущенных приложений» и «Целостность файлов пользователей».

## А в вашем Dr.Web включена эта настройка?

В случае наличия подключения ПК к Интернету Превентивная защита получает знания о наиболее актуальных алгоритмах противодействия неизвестным угрозам из облачного онлайн-сервиса Dr.Web Cloud. Это обеспечивает защиту от вредоносных программ, попавших к аналитикам Dr.Web уже после того, как антивирус на вашем компьютере получил последнее обновление.

Как правило, традиционные обновления попадают на компьютер не чаще чем раз в час. А в Dr.Web Cloud информация всегда актуальна, так как добавляется в него сразу после того, как станет известна аналитикам Dr.Web. Использование базы знаний облака существенно повышает защиту от угроз, использующих уязвимости «нулевого часа».

## А в вашем Dr.Web включено Облако Dr.Web?

По умолчанию в Превентивной защите Dr.Web установлен **Оптимальный** уровень защиты. Подробнее о настройках Превентивной защиты Dr.Web написано [здесь](#).

Превентивная защита имеет систему профилей, с помощью которых можно создавать гибкие правила для доверенных приложений и тем самым не допустить возникновения конфликтов при работе Превентивной защиты Dr.Web. Подробнее о настройках профилей Превентивной защиты Dr.Web написано в [документации](#).

## Защита от потери данных должна быть включена и настроена

**«Защита от потери данных» сохраняет самые важные файлы пользователя в специальном защищенном Dr.Web хранилище.**

В отличие от обычных программ резервного копирования, Dr.Web создает и защищает от несанкционированного доступа злоумышленников хранилище с копиями файлов. Даже если новейший (пока неизвестный Dr.Web) троянец все-таки проникнет на ваш ПК, использование «Защиты от потери данных» спасет ваши файлы. И даже если троянец все-таки зашифрует ваши файлы, вы сможете восстановить их самостоятельно, без обращения в службу техподдержки «Доктор Веб».

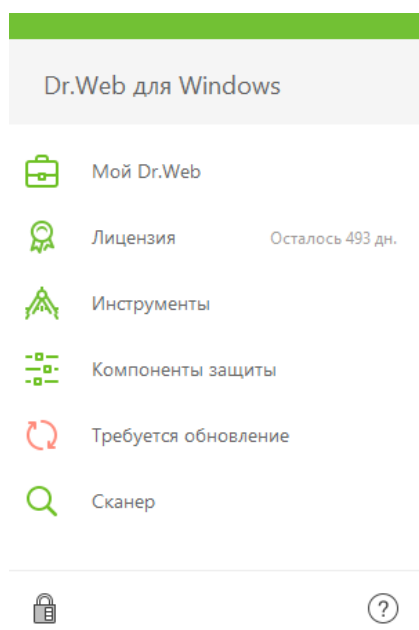
По умолчанию этот компонент не включен, потому что для его работы требуется указать данные, которые необходимо сохранять, а также настроить места и способ хранения данных.

## А в вашем Dr.Web включена и настроена ли «Защита от потери данных»?

## Лицензия Dr.Web должна быть актуальной

**Чтобы Dr.Web защищал ваш ПК, лицензия должна быть активной (действующей).**

После истечения срока действия лицензии все компоненты защиты Dr.Web перестают работать.



### Чтобы узнать сроки действия вашей лицензии Dr.Web

Кликните на значок  в системном трее. Если лицензия действующая, вы увидите в открывшемся меню количество дней, оставшихся до конца срока действия лицензии.

Сроки действия лицензии Dr.Web также можно узнать в [Менеджере лицензий на сайте](#).

## А в вашем Dr.Web сейчас действующая лицензия?

# Правила поведения в случае заражения шифровальщиком

Чтобы восстановление зашифрованных файлов специалистами «Доктор Веб» было возможным, пользователю НЕЛЬЗЯ:

- менять расширение у зашифрованных файлов;
- переустанавливать операционную систему;
- самостоятельно использовать какие-либо программы для расшифровки/восстановления данных;
- удалять/переименовывать какие-либо файлы и программы (в том числе временные);
- предпринимать необратимые действия по лечению/удалению вредоносных объектов.

В результате этих действий вы можете окончательно потерять свои данные — их не сможет найти и восстановить даже специальная утилита расшифровки.

Поэтому лучше не предпринимайте никаких действий с зараженным компьютером до получения ответа от «Доктор Веб» о возможности восстановления файлов.

[Правила поведения в условиях заражения троянцем-вымогателем](#)

[Образцы заявлений в полицию](#)

# Бесплатное восстановление файлов, зашифрованных троянцем-вымогателем

Бесплатное восстановление файлов, зашифрованных троянцем-вымогателем, производится для владельцев действующих коммерческих лицензий [Dr.Web Security Space](#), [Dr.Web Enterprise Security Suite](#) (Комплексная защита) и подписчикам услуги «Антивирус Dr.Web» (тарифный пакет [Dr.Web Премиум](#)) — при соблюдении ими этих [условий](#) на момент инцидента.

Для пользователей других антивирусов услуга платная — для этого требуется приобрести лицензию на Dr.Web Rescue Pack.

## Состав лицензии

- Утилита расшифровки
- Лицензия Dr.Web Security Space для 1 ПК на 2 года

## Запрос на расшифровку

## Знания — мощное оружие против троянцев-шифровальщиков

Как правильно настроить систему защиты от троянцев-вымогателей, рассказывает обучающий курс **DWCERT-070-6 «Защита рабочих станций и файловых серверов Windows от действий программ-шифровальщиков»**, который можно скачать по ссылке <https://training.drweb.ru/users>.

## Кругом обман? Но есть «Антивирусная правДА!»

О том, как бороться с троянцами-шифровальщиками, читайте на страницах просветительского проекта «Антивирусная правДА!», в рубрике «Закодировать всё».

|  Закодировать всё                        |  Закодировать всё                        |  Закодировать всё                      |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 08.02.2016                                                                                                                  | 24.02.2016                                                                                                                  | 25.02.2016                                                                                                                  |
| Платить ли выкуп вымогателям? Вот в чем вопрос!                                                                             | Возможна ли защита от троянцев-шифровальщиков?                                                                              | Все пропало! Как быть?                                                                                                      |
| Прочитали: 41332<br>Оценили: +195 -2<br>Комментариев: 154<br>Рейтинг: 345<br>Поделиться: 150 раз<br>Добавили в избранное: 9 | Прочитали: 32289<br>Оценили: +173 -0<br>Комментариев: 137<br>Рейтинг: 319<br>Поделиться: 146 раз<br>Добавили в избранное: 5 | Прочитали: 29665<br>Оценили: +159 -0<br>Комментариев: 139<br>Рейтинг: 310<br>Поделиться: 151 раз<br>Добавили в избранное: 8 |

Все выпуски рубрики [«Закодировать всё»](#)

# Правила гигиены

Шифровальщики массово распространяются по почте — якобы от имени налоговой инспекции, суда и даже ваших знакомых, под видом резюме, бухгалтерских документов и пр. Если вы получили подозрительное письмо с вложением, на которое не отреагировал Dr.Web, в нем может оказаться шифровальщик, еще не известный антивирусу.

Отправьте это вложение на анализ в антивирусную лабораторию «Доктор Веб» <https://vms.drweb.ru/sendvirus> и дождитесь ответа специалиста.

Этим вы поможете не только себе (не допустите шифрования данных), но и тысячам потенциальных жертв киберпреступников.

## **Вы можете помочь остановить киберпреступников**

Шифрование данных — опасная угроза, а испорченные файлы — серьезная проблема. Но бороться с этим можно и нужно. Мы убедительно просим вас, как пострадавшую сторону, обратиться с заявлением по факту несанкционированного доступа к вашему компьютеру, распространения вредоносных программ и вымогательства в территориальное управление «К» МВД РФ. Образцы заявлений, а также ссылка на госпортал («Порядок приема сообщений о происшествии в органах внутренних дел РФ») есть на нашем сайте: <http://legal.drweb.com/templates>.

## О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

### Обучение

[Кабинет заочника](#) Dr.Web (требуется регистрация)

[Курсы для инженеров](#) | [Курсы для пользователей](#) | [Брошюры](#)

### Просвещение

[«Антивирусная правДА!»](#) | [ВебIQметр](#) | [Брошюры](#)

### Контакты

Центральный офис ООО «Доктор Веб»

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а

[Телефоны](#)

[Схема проезда](#)

[Контакты для прессы](#)

[Офисы за пределами России](#)

[антивирус.пф](#) | [www.drweb.ru](#) | [free.drweb.ru](#) | [www.av-desk.ru](#) | [curenet.drweb.ru](#)



© ООО «Доктор Веб»,  
2003-2017



Присоединяйтесь к нам в социальных сетях

