

DWCERT-070-6

Защита рабочих станций и файловых серверов Windows
от действий программ-шифровальщиков



Содержание

1. В чем особенность (опасность) программ-шифровальщиков?	3
2. Особенности настройки антивирусного ПО для защиты от действий программ-шифровальщиков	8
2.1. Установка пароля	10
2.2. Настройка действий Dr.Web Security Space с вредоносными файлами	10
2.3. Настройка системы обновлений Dr.Web Security Space	14
2.4. Настройка компонента Dr.Web Cloud	17
2.5. Включите проверку зашифрованного трафика	18
2.6. Настройка параметров Dr.Web Security Space, обеспечивающих обнаружение ранее неизвестных вредоносных файлов	20
2.7. Функционал «Защита от потери данных»	31
2.8. Ограничение возможности проникновения шифровальщиков на компьютер	32
2.8.1. Использование Офисного/Родительского контроля	32
2.8.2. Использование Брандмауэра	45
2.8.1.1. Ограничение прав сетевых приложений	47
2.8.1.2. Настройка параметров работы известных сетей	50
3. Типичные ошибки в настройке системы защиты	52
3.1. Версия антивируса	52
3.2. Отключения компонентов	53
3.3. Отказ от обновлений	55
3.4. Исключения из проверки	56
4. Рекомендации компании «Доктор Веб» по защите компьютера от программ-шифровальщиков	58
4.1. Правила действий при инциденте с шифровальщиком	59
4.2. Типичные ошибки при обнаружении действий шифровальщика и обращении в службу технической поддержки	60
4.3. Включение показа расширений имен файлов	61
4.4. Утилиты дешифровки	62
4.5. Где могут находиться файлы программ-шифровальщиков	63

Дополнительная информация

Просветительский проект	«Троянцы — шифровальщики — Угроза №1»
«Антивирусная правда!»	Рубрика «Закодировать все», а также другие выпуски с хэштегами #Trojan.Encoder, #шифровальщик, #вымогательство и #расшифровка
Тесты ВебиQметра	Закодировать все, или Резюме Trojan.Encoder Закодировать всё — 2, или Криптография на службе криминала Закодировать всё — 4, или Спасайся кто может Закодировать всё — 3, или Гоните ваши денежки — иначе быть беде
Листовка	«Троянцы-шифровальщики — угроза №1»
Видео	Настройка «Защиты от потери данных»
Вирусная библиотека	Описания троянцев семейства Trojan.Encoder

1. В чем особенность (опасность) программ-шифровальщиков?

На данный момент одной из основных проблем, с которой сталкиваются администраторы локальных сетей и отдельные пользователи, являются действия программ-шифровальщиков — троянцев семейства Trojan.Encoder.

Внимание! В последнем квартале ушедшего года число заражений шифровальщиками увеличилось более чем вдвое — с 9 до 20%, опередив в рейтинге шпионское ПО. При этом количество заражений майнерами — наиболее популярными вредоносными программами 2018 года — упало с 15 до 8%.

Злоумышленники разочаровавшись в майнерах и снова переключаются на шифровальщиков.

Троянцы-шифровальщики (Trojan.Encoder) — вредоносные программы, которые отыскивают на дисках инфицированного компьютера, локальной сети или в памяти мобильного устройства пользовательские файлы, после чего шифруют их и требуют у жертвы выкуп за расшифровку. Кроме непосредственно шифровальщиков функционал шифрования пользовательских файлов имеют и вредоносные программы иного назначения. Так, например, майнеры в случае обнаружения могут начать шифровать файлы в целях дальнейшего получения выкупа.

Внимание! Если вы получили требование о выкупе — не связывайтесь со злоумышленниками. В более чем 50% случаев после оплаты вы не получите дешифратор и потеряете деньги.

Внимание! Даже если вы заплатите выкуп злоумышленнику и/или вам будет продемонстрирована возможность расшифровки, никакой гарантии восстановления информации это вам не дает.

Trojan.Encoder.11432 (он же WannaCry, WannaCryptor, WanaCrypt0r, WCrypt, WCRY и WNCRY) шифрует файлы с использованием алгоритма AES, при этом используется два режима — тестовый и обычный. В тестовом режиме шифрование производится с помощью зашитого в троянце ключа. Этим режимом шифруются файлы, возможность расшифровки которых демонстрируется пользователю. Поэтому расшифровка зашифрованных в тестовом режиме данных возможна даже без помощи злоумышленников. А вот остальные файлы шифруются другим ключом, и возможность их расшифровки пользователю не демонстрируется.

Опрос представителей более 1200 ИТ фирм в 17 странах мира показал, что

Заплатить преступникам решили 38,7% компаний, но только чуть меньше половины из них (19,1%) в итоге получили от операторов малвари инструменты для расшифровки данных. Оставшиеся 19,6% лишились одновременно и денег, и информации.

<https://xakep.ru/2018/04/02/meganews-228>

Статистика говорит, что менее половины из заплативших (и даже меньше) смогли достучаться до вымогателей и расшифровать данные. Киберпреступникам безразлична их репутация. Они *зарабатывают*. Кроме этого многие из вымогателей не способны создать систему восстановления.

Зафиксирован случай, когда злоумышленники сами не смогли расшифровать зашифрованные ими файлы и отправили пострадавших в службу технической поддержки компании «Доктор Веб».

от атак вымогателей пострадали более 55% опрошенных, и 61,3% из них отказались платить злоумышленникам выкуп. Восстановить файлы своими силами в итоге удалось 53,3% отказавшихся.

<https://xakep.ru/2018/04/02/meganews-228>

Защитить данные компании вполне реально — для этого нужно совсем немного. Дело в том, что

Среднестатистический хакер — это мужчина 30–35 лет, которому в руки попало ПО для взлома компьютера или смартфона. В настоящее время взлом — это, скорее, техническое преступление, а не интеллектуальное. Завладев программой для взлома, злоумышленник просто начинает ею пользоваться и все.

<https://www.securitylab.ru/news/496954.php>

Подавляющее число так называемых «хакеров» — это люди, имеющие на руках некие утилиты, но никак не высококвалифицированные хакеры. В итоге результативность атак — в большей мере «заслуга» отсутствия защиты, а не квалификации атакующих.

Немного истории

Первые троянцы-шифровальщики семейства Trojan.Encoder появились в 2009 году. За следующие пять лет число только их основных разновидностей увеличилось более чем на 1900%, и в настоящее время Trojan.Encoder имеет несколько тысяч модификаций — каждый день в антивирусную лабораторию Dr.Web попадает не менее десятка новых образцов.

```
Trojan.DownLoader24.58068 Trojan.DownLoader24.58069 Trojan.DownLoader24.58070 Trojan.DownLoader24.58071 Trojan.DownLoader24.58072
Trojan.DownLoader24.58073 Trojan.DownLoader24.58074 Trojan.DownLoader24.58075 Trojan.DownLoader24.58076 Trojan.DownLoader24.58077
Trojan.DownLoader24.58078 Trojan.DownLoader24.58079 Trojan.DownLoader24.58080 Trojan.DownLoader24.58081 Trojan.DownLoader24.58082
Trojan.DownLoader24.58083 Trojan.DownLoader6.34128 Trojan.Emotet.135 Trojan.Emotet.136 Trojan.Encoder.10193 Trojan.Encoder.10317 Trojan.Encoder.10507
Trojan.Encoder.10710 Trojan.Encoder.10731 Trojan.Encoder.10927 Trojan.Encoder.10994 Trojan.Encoder.10998 Trojan.Encoder.11011 Trojan.Encoder.11198(2)
Trojan.Encoder.11320(8) Trojan.Encoder.11372(2) Trojan.Encoder.11373 Trojan.Encoder.11374 Trojan.Encoder.11375 Trojan.Encoder.11376
Trojan.Encoder.11377 Trojan.Encoder.11378 Trojan.Encoder.11379 Trojan.Encoder.11380 Trojan.Encoder.11381 Trojan.Encoder.11382 Trojan.Encoder.11383
Trojan.Encoder.11384 Trojan.Encoder.11385 Trojan.Encoder.11386 Trojan.Encoder.11387 Trojan.Encoder.11388 Trojan.Encoder.11389 Trojan.Encoder.11390
Trojan.Encoder.11391 Trojan.Encoder.11392 Trojan.Encoder.11393 Trojan.Encoder.11394 Trojan.Encoder.11395 Trojan.Encoder.11396 Trojan.Encoder.11397
Trojan.Encoder.11398 Trojan.Encoder.11399 Trojan.Encoder.11400 Trojan.Encoder.11401 Trojan.Encoder.11402 Trojan.Encoder.11403 Trojan.Encoder.11404
Trojan.Encoder.11405 Trojan.Encoder.11406 Trojan.Encoder.11407 Trojan.Encoder.11408 Trojan.Encoder.11409 Trojan.Encoder.11410 Trojan.Encoder.11411
Trojan.Encoder.11412 Trojan.Encoder.11413 Trojan.Encoder.11414 Trojan.Encoder.11415 Trojan.Encoder.11416 Trojan.Encoder.11417 Trojan.Encoder.11418
Trojan.Encoder.11419 Trojan.Encoder.11420 Trojan.Encoder.11421 Trojan.Encoder.11422 Trojan.Encoder.11423 Trojan.Encoder.11424 Trojan.Encoder.11425
Trojan.Encoder.11426 Trojan.Encoder.11428 Trojan.Encoder.11429 Trojan.Encoder.11430 Trojan.Encoder.11431 Trojan.Encoder.11432 Trojan.Encoder.11433
Trojan.Encoder.3453 Trojan.Encoder.4691 Trojan.Encoder.7074(2) Trojan.Encoder.7111(2) Trojan.Encoder.726 Trojan.Encoder.727 Trojan.Encoder.728(3)
Trojan.FakeAlert.49828 Trojan.FakeAlert.49830(4) Trojan.FakeAlert.49835(2) Trojan.FakeAlert.54848(2) Trojan.FindStr.27 Trojan.FindStr.28
Trojan.Fayna.2848 Trojan.Gozi.20(5) Trojan.Hosts.42041 Trojan.Hosts.42042 Trojan.Hosts.42043 Trojan.Hosts.5285 Trojan.Inject1.45089
Trojan.Inject1.45089 Trojan.Inject2.25433(1) Trojan.Inject2.27023 Trojan.Inject2.28753 Trojan.Inject2.43784 Trojan.Inject2.43785 Trojan.Inject2.43786
```

Шифровальщики, добавленные в антивирусную базу Dr.Web 12 мая 2017 г. — в день начала атаки Trojan.Encoder.11432 (WannaCry)

Троянцы-шифровальщики существуют не только для ПК (операционных систем MS Windows и Linux), но и для мобильных устройств.

Как правило, троянцы-шифровальщики обнаруживают на компьютере и/или в локальной сети файлы с определенными расширениями (например, но не только: *.mp3, *.doc, *.docx, *.pdf, *.jpg, *.rar) и шифруют их.

Отдельные представители семейства могут шифровать и иные файлы. Восстановление файлов, которые успел зашифровать троянец, является непростой задачей. Иногда файлы расшифровываются путем подбора паролей-ключей к используемым видам шифрования, но достаточно часто шифровальщики используют самые стойкие методы шифрования. Некоторые вирусы-шифровальщики требуют месяцев непрерывной дешифровки ([Trojan.Encoder.567](#)), а другие ([Trojan.Encoder.283](#)) и вовсе не поддаются корректной расшифровке.

Чтобы для результатов работы Trojan.Encoder.741 подобрать ключи вручную, нужен 107902838054224993544152335601 год.

Однако расшифровка возможна — в связи с тем, что злоумышленники, создающие вредоносные файлы, не являются специалистами ни по шифрованию, ни по работе с файлами, содержащими важную информацию.

Trojan.Encoder.11432 (WannaCry)

- Перезаписывает случайными данными файлы, если они расположены в каталогах «Рабочий стол» и «Мои документы» (в важных, с точки зрения злоумышленника, местах), а вот файлы из остальных мест переносятся во временную папку %TEMP%\%d.WNCRYT и просто удаляются с диска без перезаписи — их можно восстановить с помощью специальных программ.
- Ошибка при обработке файлов только для чтения в шифровальщике WannaCry привела к тому, что он не может шифровать подобные файлы – он создает их зашифрованные копии, а оригинальные версии не удаляются и не перемещаются. Такие файлы только получают атрибут скрытых и получить доступ к ним можно, включив отображение скрытых файлов.

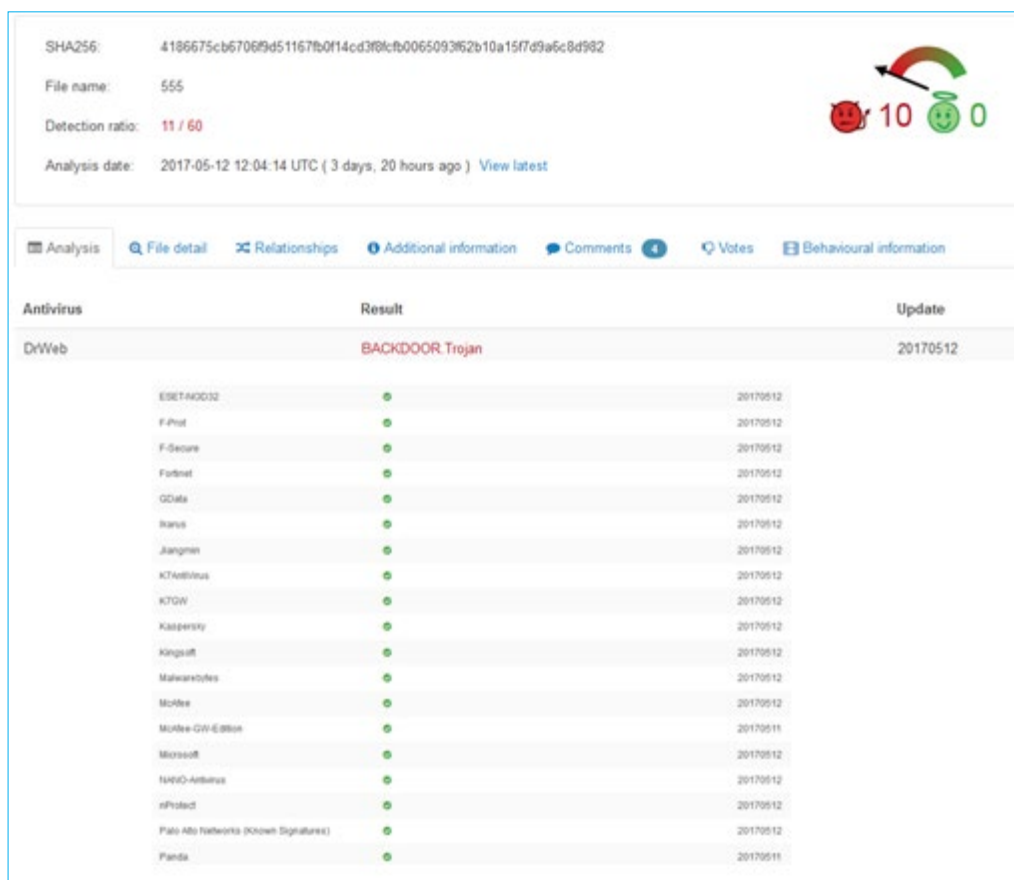
Внимание! Если ваши файлы зашифрованы и утилиты дешифровки не существует — не удаляйте их. Бывает, что алгоритм расшифровки удается найти через некоторое время.

Основная проблема, связанная с современными вредоносными программами, относится к системе их разработки: производится тестирование создаваемых вредоносных программ на обнаружение актуальными антивирусными решениями.

В результате до попадания на анализ в антивирусные лаборатории и выпуска обновлений данные вредоносные программы не обнаруживаются (в том числе с помощью эвристических механизмов), пока антивирус не получит обновления.

К счастью, злоумышленники мало осведомлены о возможностях антивирусов и зачастую проверяют возможность обнаружения на популярных сервисах, подобных Virustotal, определяющих вредоносные программы исключительно с помощью возможностей вирусных баз, без использования превентивной защиты.

Антивирус Dr.Web успешно удаляет любые известные варианты троянцев-шифровальщиков и позволяет обезвреживать в том числе даже еще не попавшие в антивирусную лабораторию модификации.



SHA256: 4186675cb6706f9d51167b0f14cd3f8c7b0065093f62b10a15f7d9a6c8d982

File name: 555

Detection ratio: 11 / 60

Analysis date: 2017-05-12 12:04:14 UTC (3 days, 20 hours ago) [View latest](#)

Analysis | File detail | Relationships | Additional information | Comments (4) | Votes | Behavioural information

Antivirus	Result	Update
DrWeb	BACKDOOR.Trojan	20170512
ESET-NOD32	●	20170512
F-Prot	●	20170512
F-Secure	●	20170512
Fortinet	●	20170512
GData	●	20170512
Ikarus	●	20170512
Jiangmin	●	20170512
K7AntiVirus	●	20170512
K7GW	●	20170512
Kaspersky	●	20170512
Kingsoft	●	20170512
Malwarebytes	●	20170512
McAfee	●	20170512
McAfee-GW-Edison	●	20170511
Microsoft	●	20170512
NANO-Antivirus	●	20170512
nProtect	●	20170512
Palo Alto Networks (Known Signatures)	●	20170512
Panda	●	20170511

Для пользователей Dr.Web Trojan.Encoder.11432 не представлял угрозы с самого начала своего распространения. <http://news.drweb.ru/show/?i=11290>

Внимание! В любой момент времени ни одна антивирусная программа — без применения современных технологий (таких как система ограничения доступа или контроль запускаемых процессов) — не может обеспечить 100% защиту от проникновения еще не известных (не попавших на анализ аналитикам антивирусной компании) вредоносных программ.

Интересный факт: использование Антиспама Dr.Web обеспечивает удаление до 98% шифровальщиков, передающихся через электронную почту, за счет фильтрации фишинговых сообщений технологиями антиспам-ядра Dr.Web, основанными на анализе сообщений.

Более подробная информация о троянцах-шифровальщиках находится по адресу http://antifraud.drweb.ru/encryption_trojs.

2. Особенности настройки антивирусного ПО для защиты от действий программ-шифровальщиков

Троянец-шифровальщик, еще не известный системе антивирусной защиты, может проникнуть в локальную сеть или на отдельный компьютер через спам (как правило, сообщение содержит вложение или специально сформированную ссылку), с помощью сообщения мессенджера (также содержащего ссылку), с зараженного сайта, или на зараженной флешке, или через незакрытую уязвимость. Именно последнюю возможность проникновения использовал знаменитый Trojan.Encoder.11432 (WannaCry).

Вредоносная программа (в том числе шифровальщик) может быть загружена иной вредоносной программой — Downloader'ом или, как Trojan.Encoder.11432, сетевым червем. В ряде случаев заражение произойдет без участия пользователя — достаточно наличия доступа в Интернет и ошибок в конфигурации компьютера.

Внимание! Современные вредоносные программы создаются так, чтобы пользователь не замечал их работы до нужного злоумышленникам момента — пока файлы на компьютере не будут зашифрованы и/или не появится сообщение с требованием выкупа. В связи с этим само заражение вполне может произойти незаметно.

Внимание! В связи с тем, что троянцы-шифровальщики могут выводить свои требования до завершения процесса шифрования, при появлении требования о выкупе нужно немедленно выдернуть вилку из розетки, обесточив компьютер. Нельзя давать шанса шифровальщику замести следы при выключении компьютера. Ни в коем случае нельзя продолжать работу на компьютере или устройстве после обнаружения признаков активности шифровальщика.

Здравствуйтесь, открыли письмо, компьютер начал виснуть, перезагрузили через какое то время, долго включался. как включился, все было зашифровано. Сидел в интернете, смотрел новости, был в соцсети, ничего не скачивал, по ссылкам не переходил. Компьютер подтормозил и выдал баннер от Wana Decryptor с вымогательством денег. Баннер всплывал каждые 5 сек. Минут через 40 мой антивирус ... поймал друг за другом 14 Троянов.**

Запрос в техническую поддержку

** Пользователь не использовал продукты Dr.Web.*

Внимание ошибка! Типичной ошибкой при обнаружении повышенного потребления ресурсов или «торможения» системы является ее перезагрузка или иные действия по оптимизации работы системы. На самом деле потребление ресурсов системой может быть связано с работой шифровальщика.

Первым действием при обнаружении повышенного расхода ресурсов должен стать запуск антивирусного сканера, настроенного на перемещение обнаруженных вредоносных файлов в карантин!

Внимание! Небрежное отношение к защите персональных данных среди ваших знакомых и партнеров приводит к тому, что письмо с шифровальщиком может прийти от имени известного вам человека или организации — например, от налоговой инспекции или банка. Более того, письмо может быть адресовано именно получателю!

1. Если неизвестные варианты троянцев семейства Trojan.Encoder уже проникли на компьютер, то они могут быть опознаны вирусными базами и удалены не ранее, чем будет получено ближайшее обновление антивируса. Поэтому обновлять вирусные базы нужно как можно чаще — не реже чем раз в час.
2. Если вредоносная программа не известна антивирусным базам, ее запуск может быть предотвращен иными компонентами защиты — в первую очередь Превентивной защитой Dr.Web.

К сведению. Действительно, обнаружение 100% угроз нулевого дня невозможно, но тем не менее используемые технологии позволяют обнаруживать неизвестные угрозы. Так, Dr.Web Trojan.Encoder.11432 (WannaCry) обнаруживался эвристическими механизмами ядра — до момента поступления образцов на анализ в антивирусную лабораторию.




Преступники создают сотни и тысячи новых образцов вредоносных программ в день, и гарантировать, что файловый антивирус, ищущий вирусы на основе знаний, хранящихся в вирусных базах, обнаружит все варианты троянцев в момент проникновения, — наивно. Обеспечить обнаружение неизвестных представителей семейства Trojan.Encoder может **модуль Превентивной защиты**, с помощью технологий поведенческого анализатора контролирующей попытки злоумышленников выполнить нужное им действие, «на лету» сравнивая поведение запускаемых программ с поведением троянцев-шифровальщиков. Использование компонента Превентивная защита позволяет опознать проникшего троянца непосредственно после попытки его запуска — даже если в антивирусные базы еще не внесена информация о нем. Использование антивируса без Превентивной защиты — опасная ошибка.

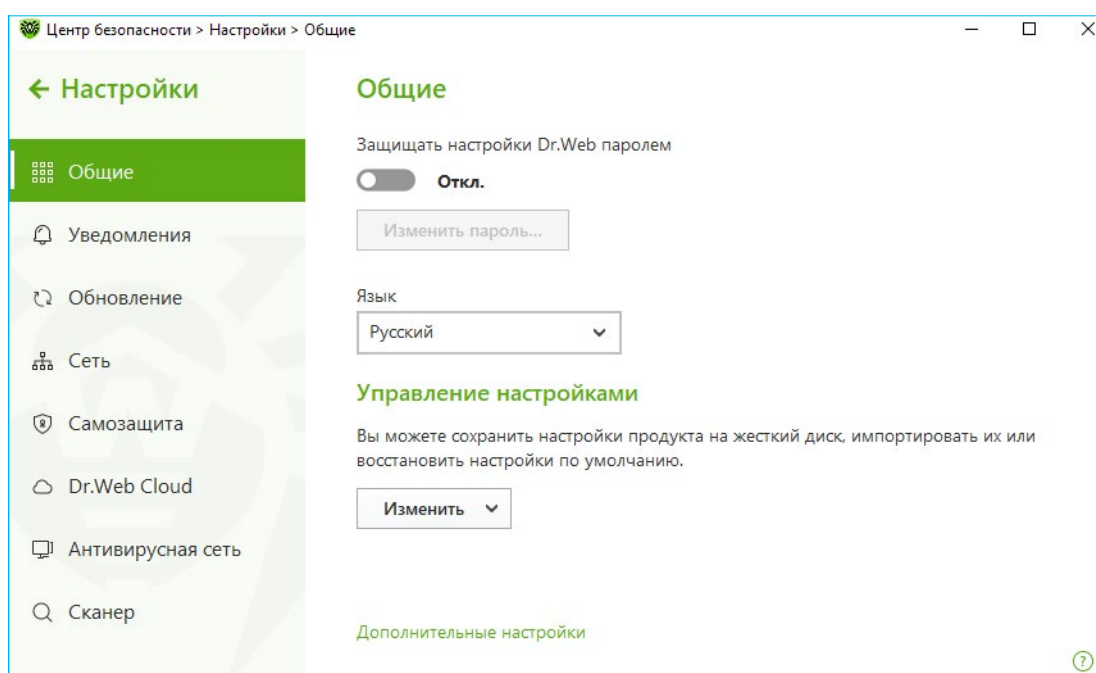
3. При наличии доступа в Интернет включите использование компонента **Dr.Web Cloud** (он есть в продуктах **Dr.Web Security Space** (для Windows), **Dr.Web Desktop Security Suite** (для Windows), **Dr.Web Desktop Security Suite** (для Windows) (лицензия Комплексная защита), а также Dr.Web KATANA. Это позволяет находить неизвестные антивирусному ядру угрозы еще быстрее, т. к. информация о них становится доступной системе защиты до получения соответствующего обновления.
4. К сожалению, даже использование технологий поведенческого анализатора, позволяющего антивирусу обнаруживать неизвестные варианты шифровальщиков, не позволяет полностью предотвратить шифрование файлов — на компьютере с установленным Dr.Web за время анализа подозрительного процесса шифровальщик может успеть зашифровать до десятка файлов. Для предотвращения потери данных необходимо настроить компонент «Защита от потери данных», входящий в состав **Dr.Web Security Space**, а также **Dr.Web Desktop Security Suite** (для Windows), лицензия Комплексная защита.

Внимание! В связи с тем, что возможности по противодействию программам-шифровальщикам у решений **Dr.Web Security Space** и **Dr.Web Desktop Security Suite** (для Windows), лицензия Комплексная защита, одинаковы, все настройки будут рассматриваться на примере **Dr.Web Security Space**.

2.1. Установка пароля

Установка пароля позволит гарантировать невозможность отключения защиты, в том числе в случае взлома.



Для установки пароля доступа в Центре безопасности нажмите значок  (значок изменит вид на ) и, нажав на ставший зеленым значок , в правом верхнем углу окна, выберите в меню **Настройки** пункт **Общие**. Нажмите на переключатель и далее на кнопку **Изменить пароль**.

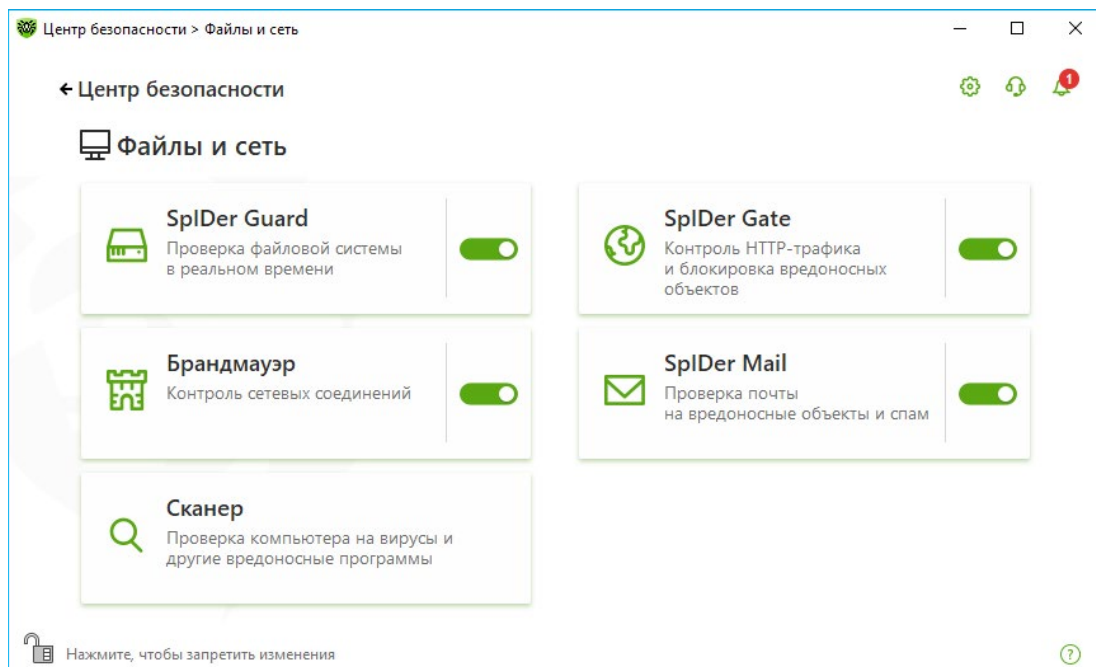


Внимание! Не рекомендуется устанавливать пароль, совпадающий с паролем доступа к компьютеру или устройству, — в случае взлома компьютера это облегчит действия злоумышленника по нейтрализации защиты.

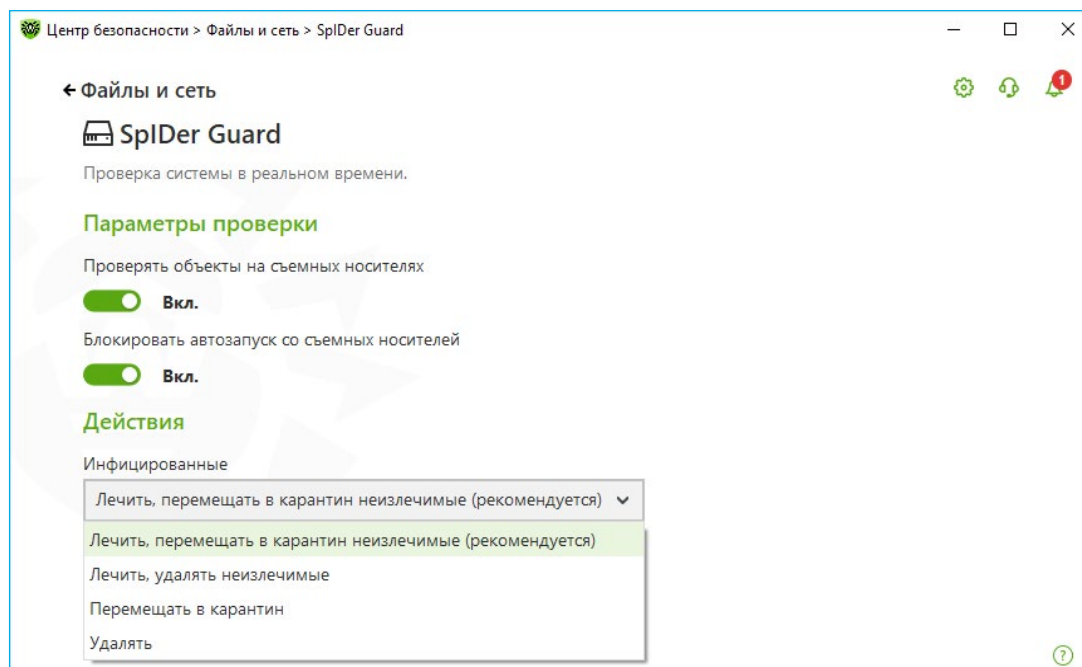
2.2. Настройка действий Dr.Web Security Space с вредоносными файлами

Внимание! Для восстановления данных из зашифрованных файлов желательно иметь сам вредоносный файл, который произвел данное действие. Кроме того, вредоносные файлы семейства Trojan.Encoder относятся к неизлечимым объектам. Поэтому по отношению к ним необходимо использовать действие «Лечить», перемещать в карантин неизлечимые.

Кликните по значку значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне последовательно нажмите на  (Режим администратора).



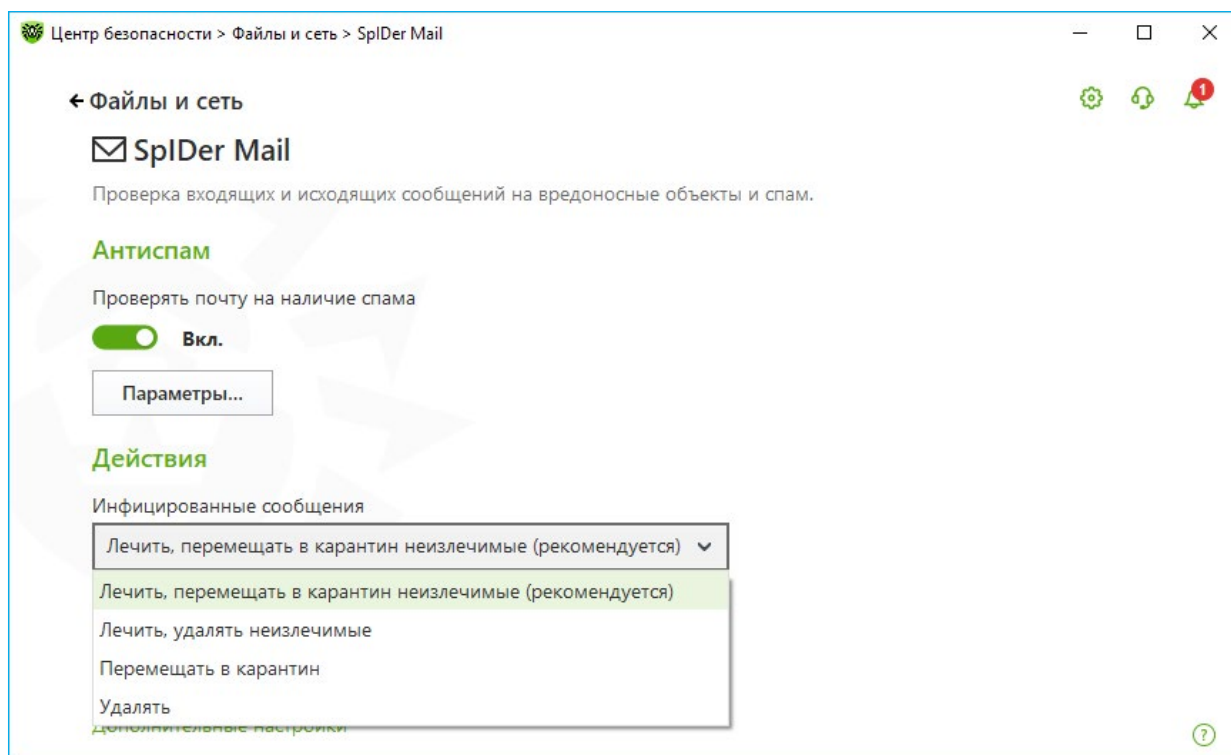
В открывшемся окне Центр безопасности выберите **Файлы и сеть** и далее **SpiDer Guard**.




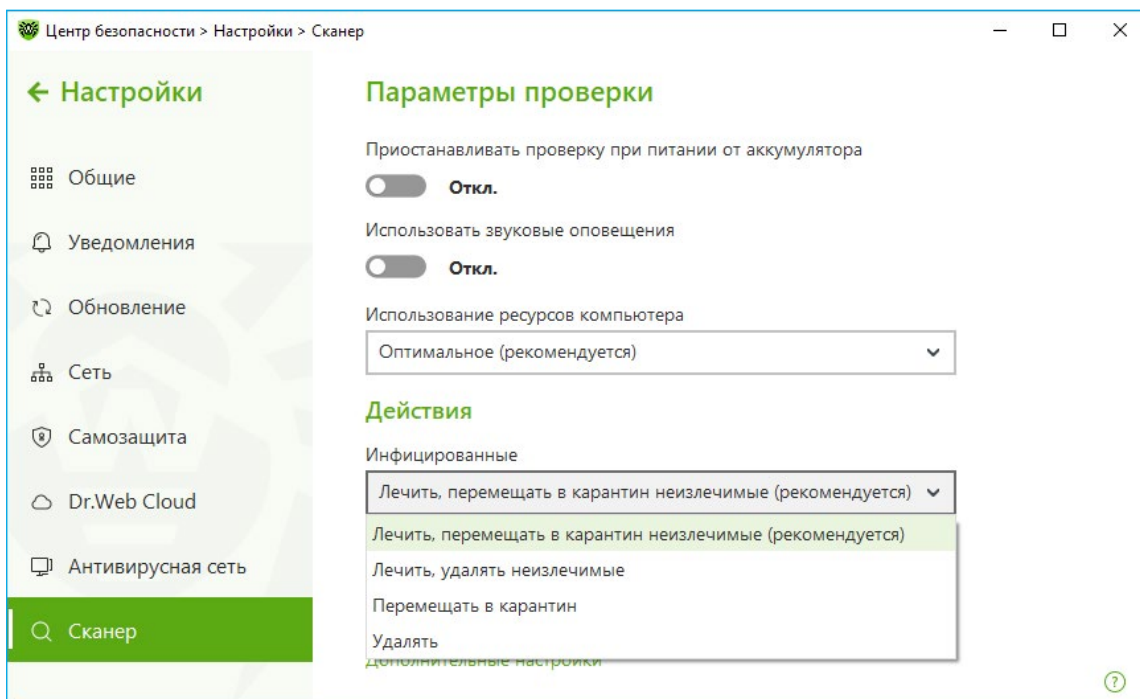
Важно! Как правило, шифровальщики относятся к таким типам вредоносных файлов, как вирусы и троянцы. Однако функция шифрования файлов также может использоваться вирусописателями и в других типах вредоносных программ. Например, в майнерах. В связи с этим не рекомендуется выставлять действие перемещения в карантин только для пунктов **Инфицированные** и **Подозрительные**. Как минимум данное действие рекомендуется выставить для пункта **Потенциально опасные**. Для доступа к данному пункту в окне **SpIDer Guard** необходимо нажать на **Дополнительные настройки**.

Аналогичные настройки необходимо установить для модуля **SpIDer Mail**, антивирусного сканера.

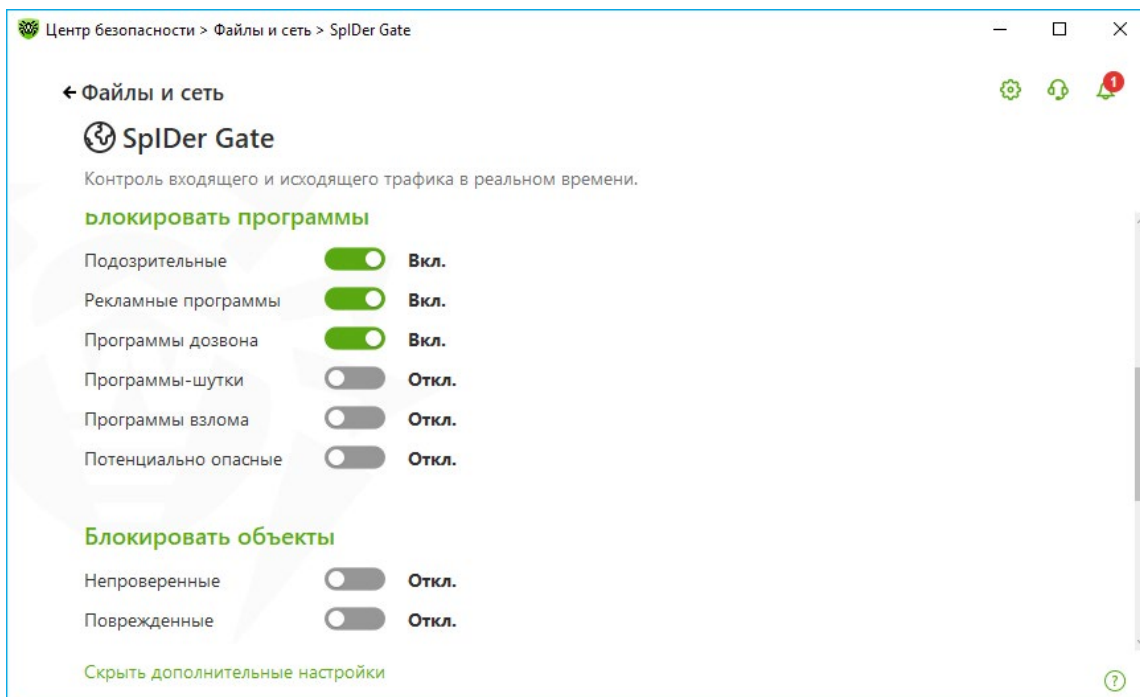
Доступ к настройке параметров **SpIDer Mail** осуществляется также из окна Центр безопасности.



Для доступа к настройкам Сканера в окне Центр безопасности необходимо нажать на кнопку  и далее выбрать пункт **Сканер**.







В окне настроек **SpiDer Gate**, также доступном из окна **Центр безопасности**, необходимо разрешить блокировку подозрительных и потенциально опасных файлов.

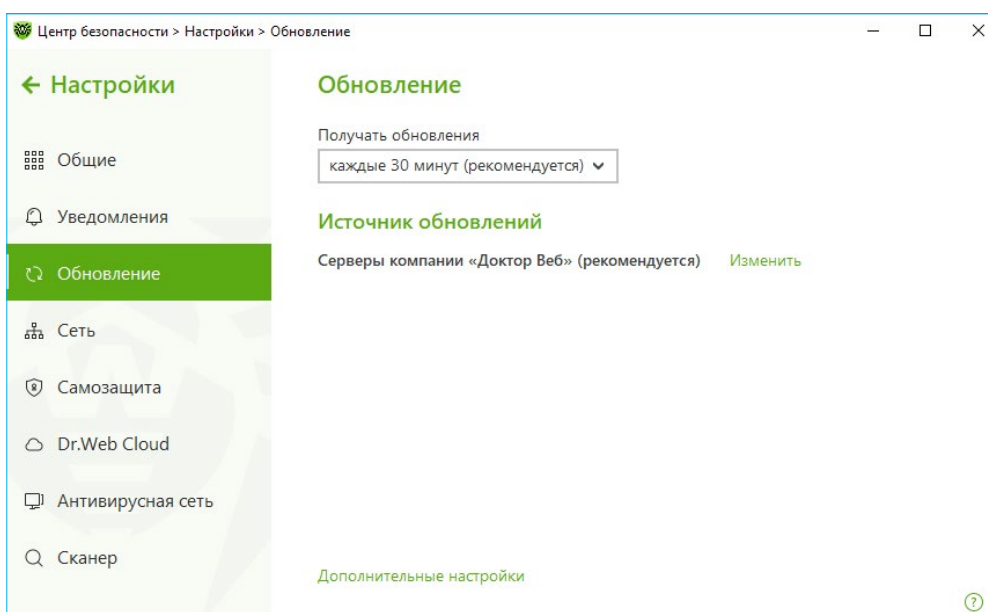


Внимание! Не удаляйте объекты из карантина, так как в некоторых случаях вредоносные файлы могут содержать ключи, которые могут помочь при расшифровке.

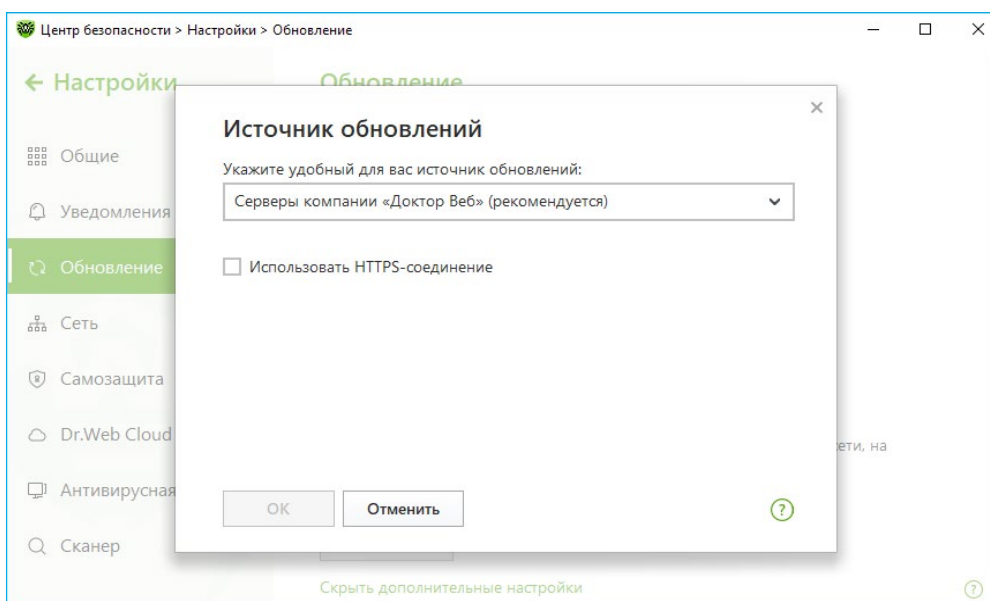
2.3. Настройка системы обновлений Dr.Web Security Space

Минимальное время заражения системы Trojan.Encoder.11432 после выхода в Интернет с открытым 445 портом — 3 минуты.

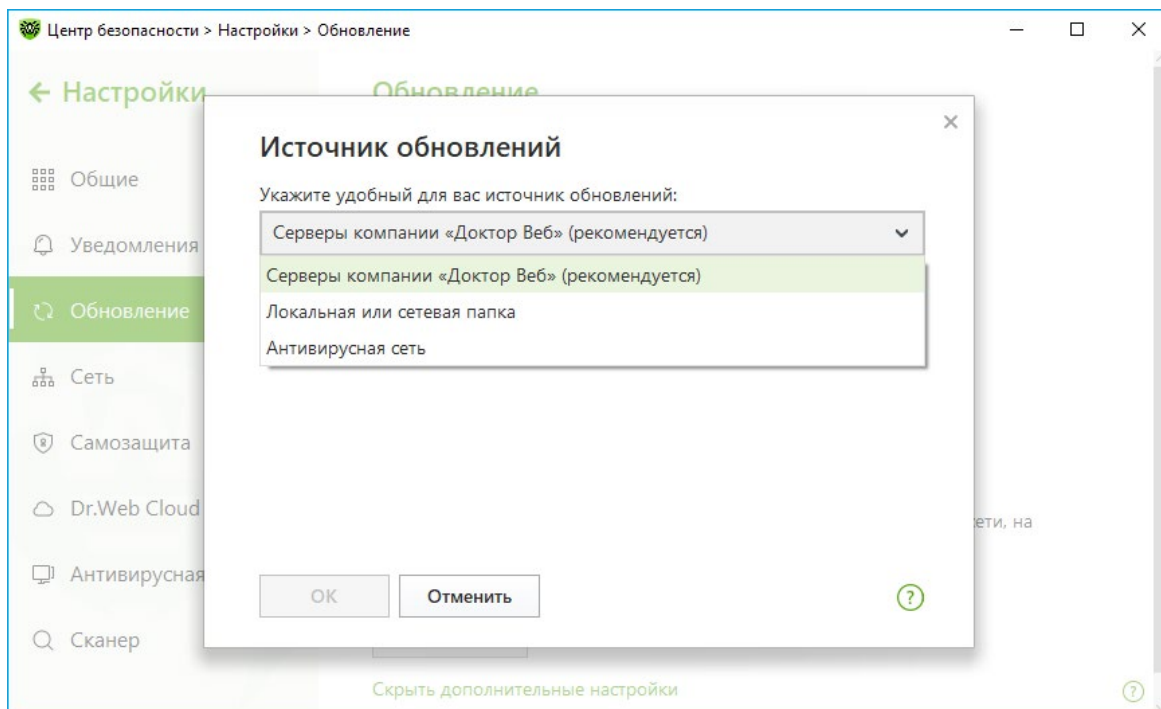
Для настройки параметров обновлений кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне последовательно нажмите на  (Режим администратора) (значок изменит вид на ) , ставший зеленым значок  в правом верхнем углу окна и выберите в меню **Настройки** пункт **Обновление**.



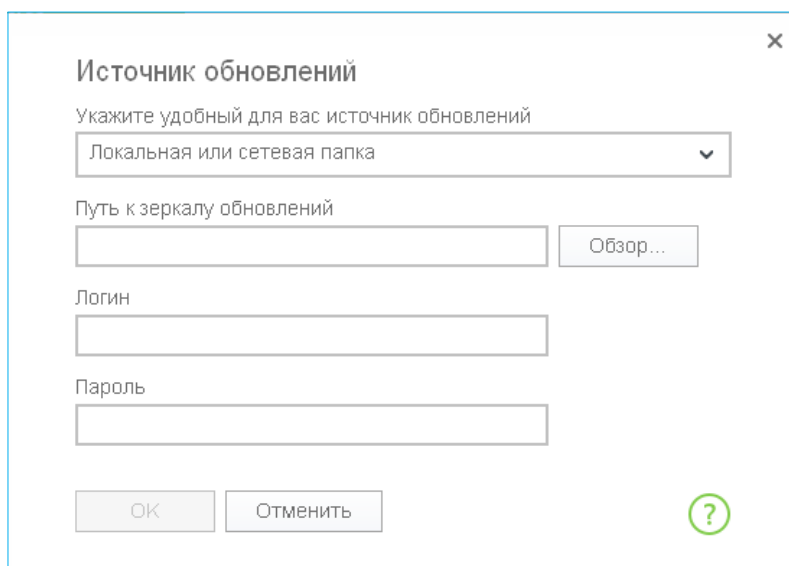
По умолчанию антивирус обновляется с серверов компании «Доктор Веб». Чтобы изменить источник обновлений, выберите **Изменить**.





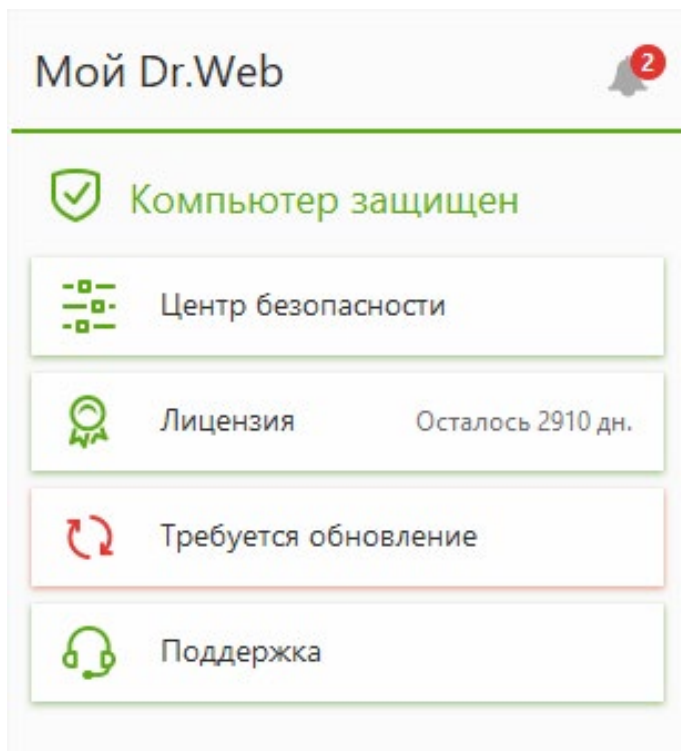
Доступны три варианта:



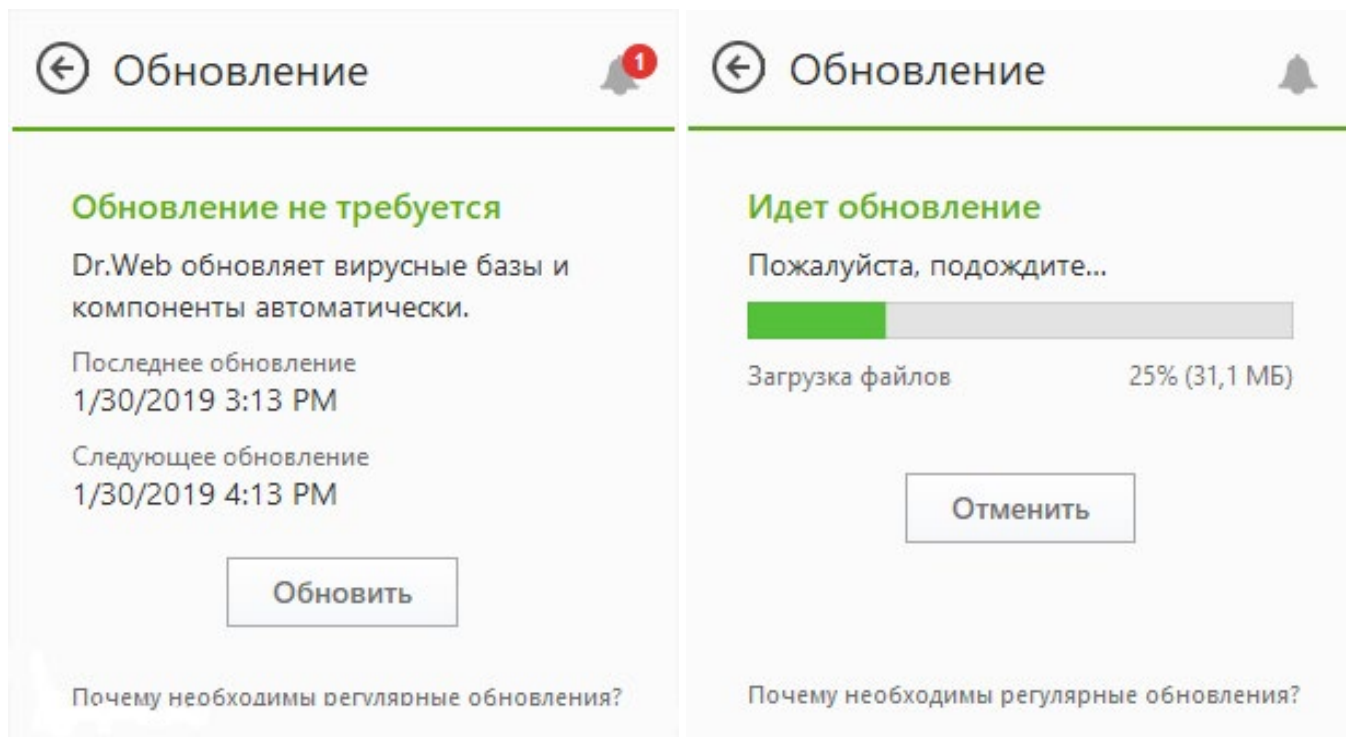
Если обновление выполняется из локальной папки, нужно указать ее адрес и параметры доступа к ней.



Чтобы провести обновление вручную или проверить статус обновлений, нажмите на значок  в системном меню, затем в открывшемся меню агента на кнопку .

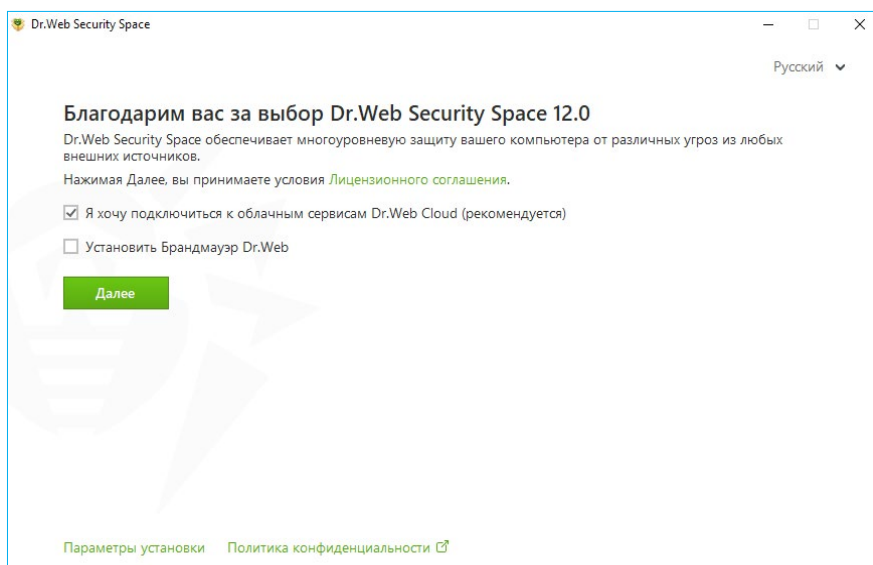






Для обновления вручную нажмите на кнопку **Обновить**.

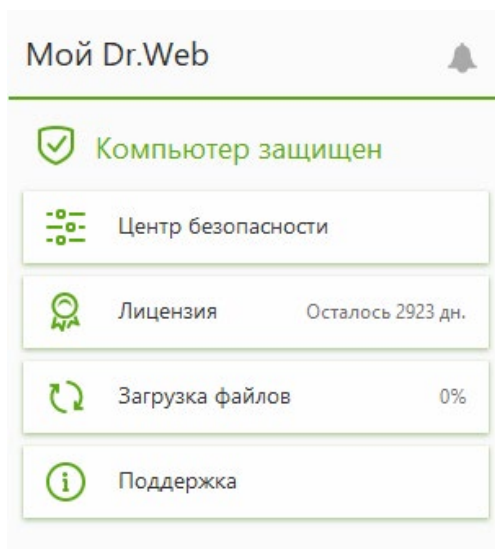


2.4. Настройка компонента Dr.Web Cloud

Использование компонента Dr.Web Cloud предлагается уже в процессе инсталляции продукта Dr.Web Security Space. Для работы компонента достаточно оставить по умолчанию значение параметра **Я хочу подключиться к облачным сервисам Dr.Web Cloud**. После завершения установки запрос репутации для каждого проверяемого объекта происходит автоматически и практически не требует расхода ресурсов защищаемого компьютера.



Если в ходе инсталляции компонент Dr.Web Cloud не был включен, кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне последовательно нажмите на  (Режим администратора) (значок изменит вид на ) и ставший зеленым значок  в правом верхнем углу окна.







В открывшемся окне **Настройки** выберите пункт меню **Основные** → **Dr.Web Cloud**.

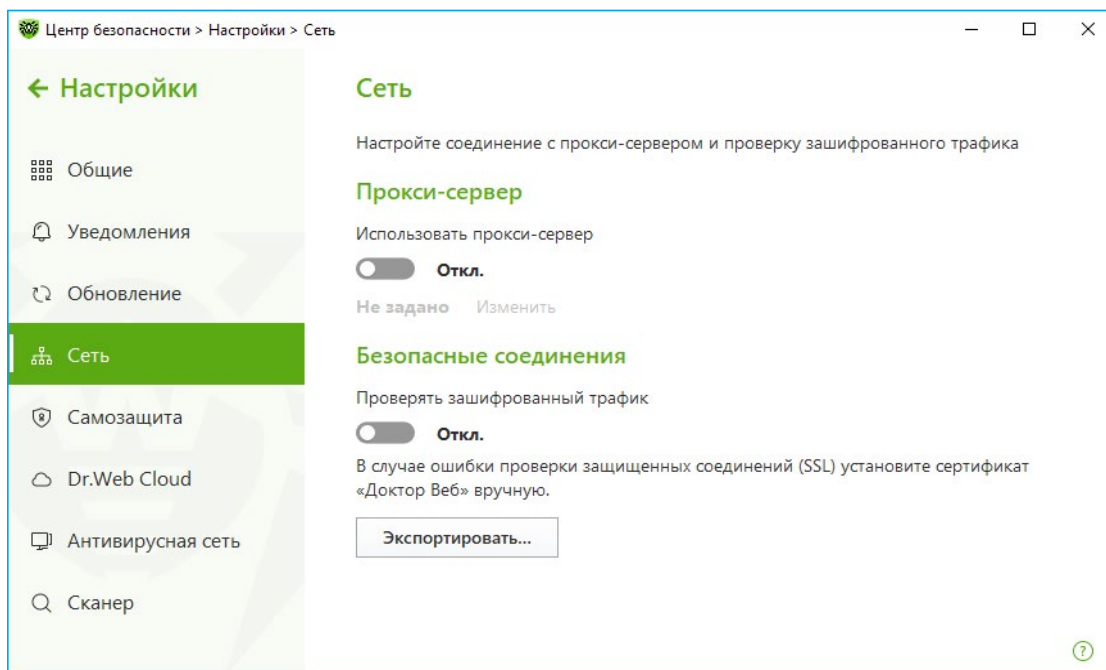


В открывшемся окне передвиньте переключатель в положение **Вкл.**

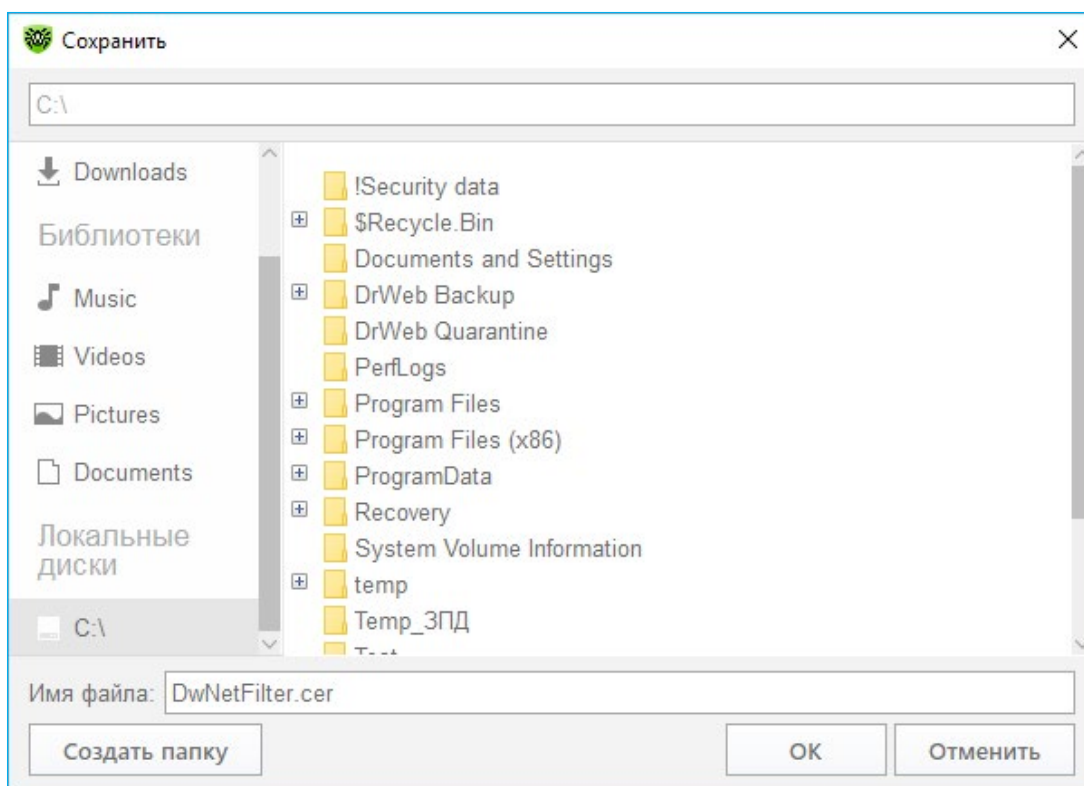
2.5. Включите проверку зашифрованного трафика

На данный момент до половины интернет-трафика зашифровано, чем могут воспользоваться злоумышленники. В связи с этим включите проверку зашифрованного трафика (функционал доступен для Dr.Web Security Space): кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне последовательно нажмите на  (Режим администратора) (значок изменит вид на ) и ставший зеленым значок  в правом верхнем углу окна.

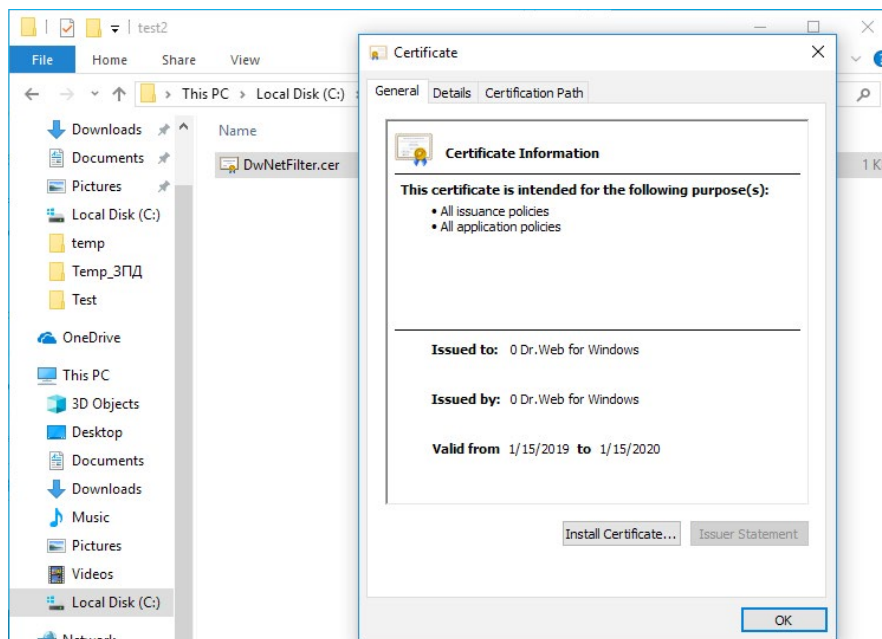
В открывшемся окне **Настройки** выберите пункт **Сеть**. Переключатель **Безопасные соединения** должен быть включен.



В случае необходимости установите сертификат Dr.Web в систему. Для этого в окне **Сеть** кликните на кнопку **Экспортировать** и сохраните предложенный файл в удобную вам папку.






Произведите установку удобным для вас способом. Например, кликнув по сохраненному файлу и подтвердив установку.

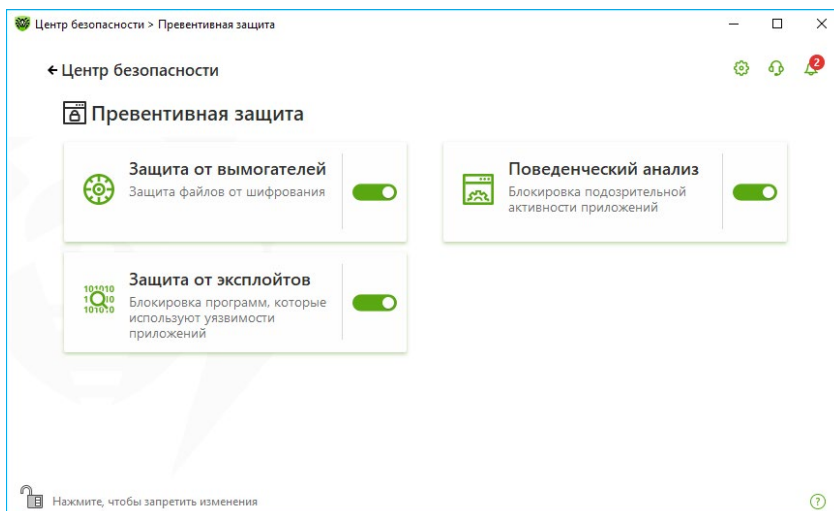


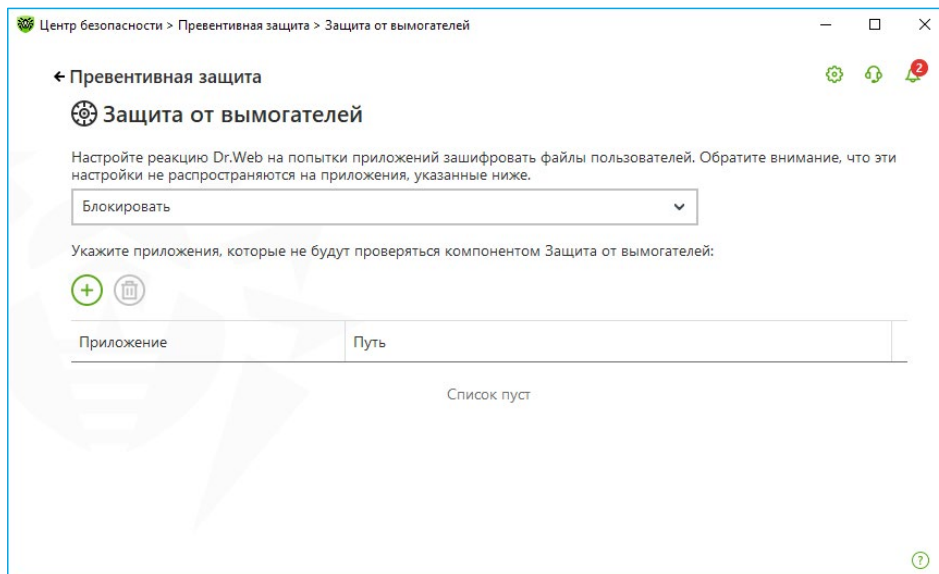
2.6. Настройка параметров Dr.Web Security Space, обеспечивающих обнаружение ранее неизвестных вредоносных файлов

Обнаружение еще не известных представителей семейства Trojan.Encoder обеспечивается в том числе модулем Превентивная защита, контролирующим попытки вредоносных программ выполнить нужное им действие, «на лету» сравнивая поведение запускаемых программ с поведением троянцев-шифровальщиков.

Для настройки параметров превентивной защиты кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку Центр безопасности и в открывшемся окне нажмите на  (Режим администратора) (значок изменит вид на ).

В окне **Центр безопасности** выберите **Превентивная защита** и далее **Защита от вымогателей**.

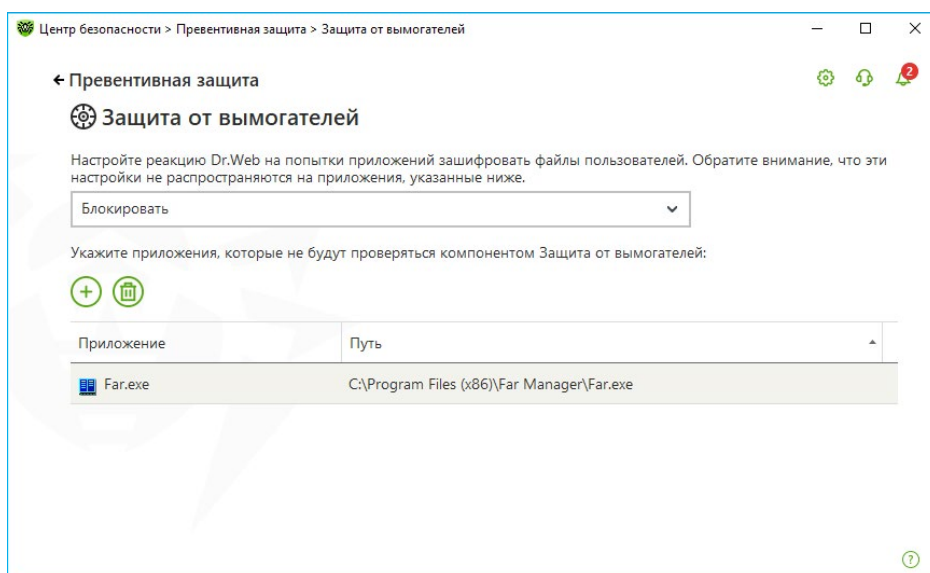




Внимание! Крайне не рекомендуется выключать данный компонент, так как многочисленные ошибки в коде троянцев-вымогателей часто повреждают файлы пользователей без возможности их восстановления.

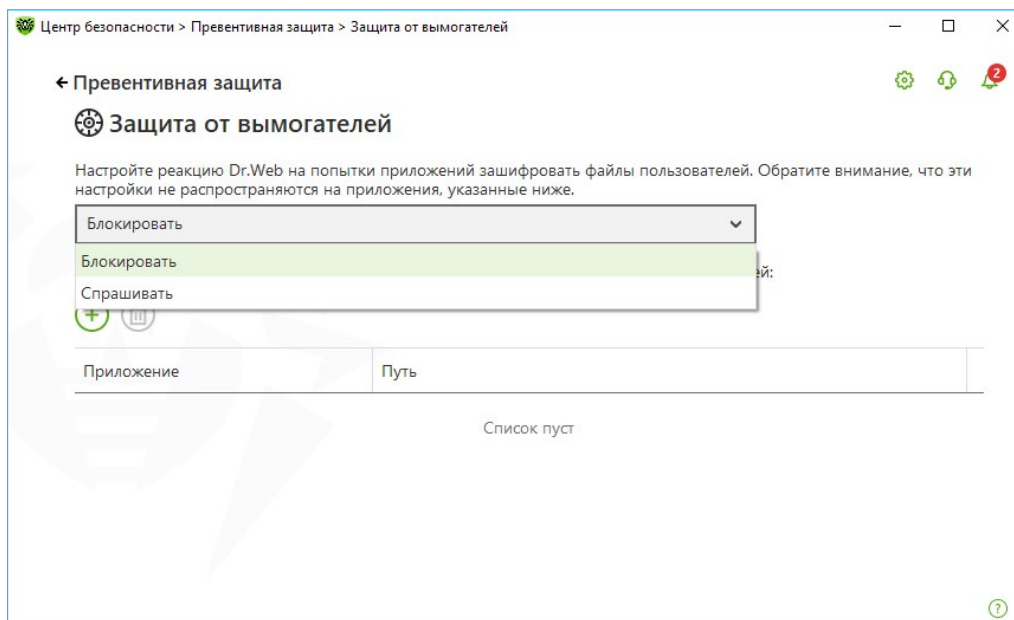
Защита от вымогателей действует на основе правил, описывающих действия, характерные для вредоносных программ, что позволяет эффективно обнаруживать угрозы, неизвестные вирусной базе.

В том случае, если вам необходимо дать полный доступ к вашим данным используемым вами программам, вы можете добавить их в список доверенных приложений. Для этого нажмите **+** и в открывшемся окне выберите программу для включения в список.

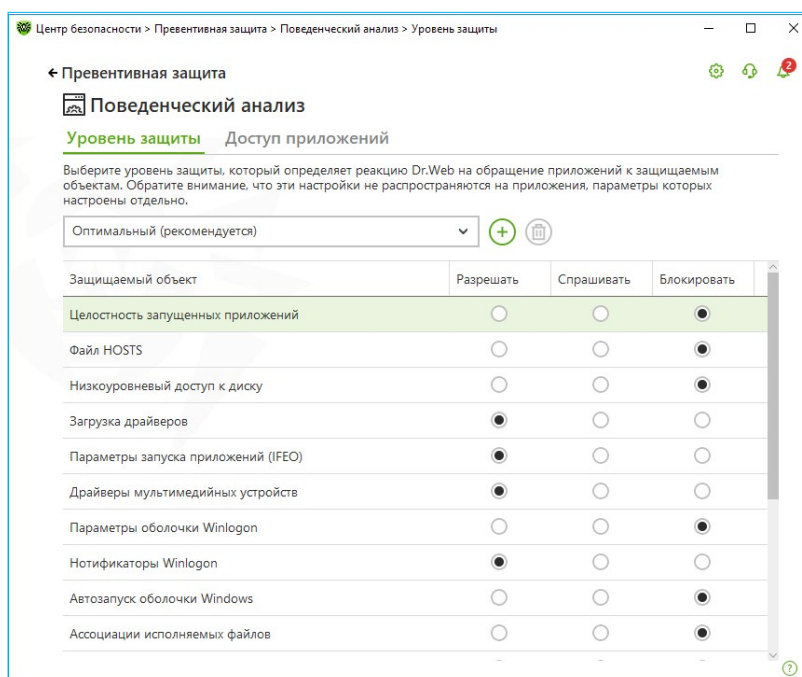


Внимание! Злоумышленники создают вредоносные приложения, имитирующие действия известных программ, или встраивают свой код в имеющиеся приложения. Известны случаи размещения взломанных приложений даже на сайтах их создателей. Поэтому крайне не рекомендуется давать полный доступ к данным без консультации с технической поддержкой Dr. Web.

Защита от вымогателей включена в Dr.Web с реакцией **Блокировать**. Вы можете изменить реакцию на **Спрашивать**. Будьте внимательны! В этом случае при каждом срабатывании системы защиты вам потребуется самостоятельно принять решение о том, является ли программа, обратившаяся к вашему файлу, вредоносной или нет.



Чтобы настроить реакцию антивируса на действия сторонних приложений, которые могут привести к заражению вашего компьютера, вернитесь в окно **Превентивная защита** и, выбрав **Поведенческий анализ**, установите необходимый уровень блокировки подозрительных действий.



Настройка данных параметров Превентивной защиты позволяет держать под контролем все попытки изменения критических областей Windows. В частности, настройки Превентивной защиты не должны позволять внедрение эксплоитов в работающие приложения.

■ **Файл HOSTS**

Этот файл позволяет определить соответствие между доменным именем хоста и его IP-адресом. Приоритет обработки файла HOSTS выше, чем приоритет обращения к DNS-серверу.

Файл HOSTS позволяет злоумышленникам блокировать доступ к сайтам антивирусных компаний и перенаправлять пользователей на поддельные сайты.

Превентивная защита Dr.Web не дает возможность вредоносным программам вносить изменения в файл HOSTS и перенаправлять пользователей на фишинговые ресурсы.

■ **Целостность запущенных приложений**

Процесс — это набор ресурсов и данных, которые находятся в оперативной памяти компьютера. Процесс, принадлежащий одной программе, не должен изменять процесс другой программы. Но вредоносные программы, например Trojan.Encoder.686 (CTB-Locker), нарушают это правило.

■ **Низкоуровневый доступ к диску**

При штатной работе операционной системы Windows доступ к файлам происходит путем обращения к файловой системе, которая подконтрольна ОС. Троянцы-буткиты, изменяющие загрузочные области диска, обращаются к диску напрямую, минуя файловую систему Windows — обращаясь к определенным секторам диска.

Внедрение троянца в загрузочную область существенно затрудняет как его обнаружение, так и процесс обезвреживания.

Превентивная защита Dr.Web блокирует возможность изменения вредоносными программами загрузочных областей диска и предотвращает запуск троянцев на компьютере.

■ **Загрузка драйверов**

Многие руткиты скрытно запускают свои драйверы и службы для маскировки своего присутствия на компьютере и выполнения несанкционированных пользователем действий, например отправки логинов и паролей, а также иных идентификационных сведений злоумышленникам.

Превентивная защита Dr.Web не дает возможности загрузки новых или неизвестных драйверов без ведома пользователя.

■ **Параметры запуска приложений**

В реестре ОС Windows существует ключ (entry) Image File Execution Options, с помощью которого для любого приложения Windows можно назначить отладчик — программу, которая помогает программисту в отладке написанного кода, в том числе позволяя модифицировать данные отлаживаемого процесса. С помощью данного ключа вредоносное ПО, будучи назначенным отладчиком какого-нибудь системного процесса или приложения (например, того же Internet Explorer или проводника), получает полный доступ к тому, что интересует злоумышленников.

Превентивная защита Dr.Web блокирует доступ к ключу реестра Image File Execution Options. Реальной необходимости отлаживать приложения «на лету» у обычных пользователей нет, а риск от использования ключа Image File Execution Options вредоносными программами очень высок.

■ **Драйверы мультимедийных устройств**

Известны некоторые вредоносные программы, которые создают исполняемые файлы и регистрируют их как виртуальные устройства.

Превентивная защита Dr.Web блокирует ветки реестра, которые отвечают за драйверы виртуальных устройств, что делает невозможным установку нового виртуального устройства.

■ **Параметры оболочки Winlogon, нотификаторы Winlogon**

Интерфейс Winlogon notification package реализует возможность обрабатывать события, назначаемые на вход и выход пользователей, включение и выключение операционной системы, и некоторые другие. Вредоносные программы, получив доступ к Winlogon notification package, могут перезагружать ОС, выключать компьютер, препятствовать входу пользователей в рабочую среду ОС. Так поступают, например, Trojan.Winlock.3020, Trojan.Winlock.6412.

Превентивная защита Dr.Web запрещает изменение веток реестра, отвечающих за Winlogon notification package, и не дает вредоносным программам возможности добавлять исполнение новых задач, нужных злоумышленникам, в логику работы операционной системы.

■ **Автозапуск оболочки Windows**

Опция блокирует сразу несколько параметров в реестре Windows в ветке [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows]: например, Applnit_DLLs (заставляет Windows загружать указанные DLL каждый раз, когда запускается какая-либо программа), Applnit_DLLs (может использоваться для внедрения руткита в Windows), Run (необходим для запуска программ в минимизированном виде после запуска операционной системы), IconServiceLib (отвечает за загрузку библиотеки Icon-

CodecService.dll, которая необходима для нормального отображения рабочего стола и значков на экране).

Превентивная защита Dr.Web блокирует ряд параметров в реестре Windows, например, запрещая вирусам изменить нормальное отображение Рабочего стола или не позволяя руткиту скрыть присутствие троянца в системе.

■ **Ассоциации исполняемых файлов**

Некоторые вредоносные программы нарушают ассоциации исполняемых файлов, в результате чего программы не запускаются — или вместо нужной пользователю программы запускается программа, назначенная вредоносным ПО.

Превентивная защита Dr.Web не позволяет вредоносному ПО изменить правила запуска программ.

■ **Политики ограничения запуска программ (SRP)**

В Windows можно настроить систему ограничения запуска программ (SRP) таким образом, чтобы разрешить запуск программ только из определенных папок (например, ProgrammFiles) и запретить выполнение программ из прочих источников. Блокировка ветки реестра, отвечающей за настройку политик SRP, запрещает вносить изменения в уже настроенные политики, таким образом усиливая уже реализованную защиту.

Превентивная защита Dr.Web позволяет защитить систему от вредоносного ПО, попадающего на компьютер через почту и съемные носители — и запускающегося, например, из временного каталога. Опция рекомендуется к использованию в корпоративной среде.

■ **Плагины Internet Explorer (ВНО)**

С помощью данной настройки можно запретить установку новых плагинов для Internet Explorer путем блокирования соответствующей ветки реестра.

Превентивная защита Dr.Web защищает браузер от вредоносных плагинов, например от блокировщиков браузера.

■ **Автозапуск программ**

Запрещает изменение нескольких веток реестра, ответственных за автозапуск приложений.

Превентивная защита Dr.Web позволяет предотвратить автозапуск вредоносных программ, не давая им зарегистрироваться в реестре для последующего запуска.

■ **Автозапуск политик**

Опция блокирует ветку реестра, с помощью которой можно запустить любую программу при входе пользователя в систему.

Превентивная защита Dr.Web позволяет предотвратить автозапуск определенных программ, например анти-антивирусов.

■ **Конфигурация безопасного режима**

Некоторые троянцы отключают безопасный режим Windows для затруднения лечения компьютера.

Превентивная защита Dr.Web предотвращает отключение безопасного режима путем блокировки изменения реестра.

■ **Параметры менеджера сессий**

Опция защищает параметры диспетчера сеансов Windows — системы, от которой зависит стабильность работы операционной системы. При отсутствии такой блокировки вредоносные программы получают возможность инициализации переменных окружения, запуска ряда системных процессов, выполнения операций по удалению, перемещению или копированию файлов до полной загрузки системы и т. п.

Превентивная защита Dr.Web защищает операционную систему от внедрения вредоносных программ, их запуска до полной загрузки операционной системы — и, следовательно, до завершения запуска антивируса.

■ **Системные службы**

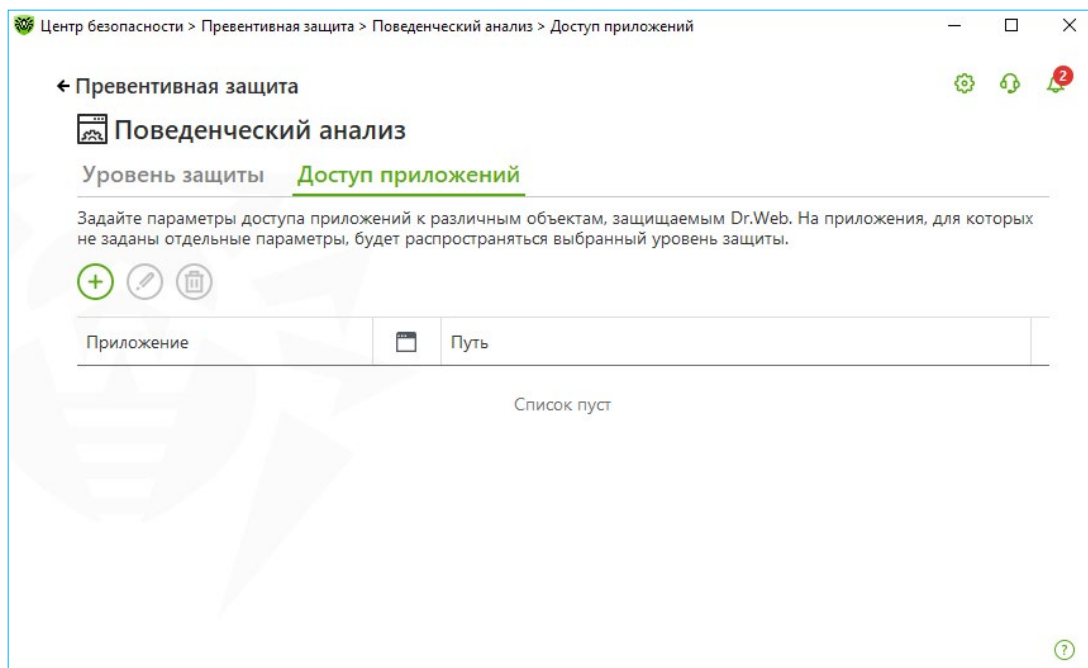
Опция защищает изменение параметров реестра, отвечающих за нормальную работу системных служб.

Некоторые вирусы могут блокировать редактор реестра, затрудняя нормальную работу пользователя. Например, очищают Рабочий стол от ярлыков установленных программ или не дают перемещать файлы.

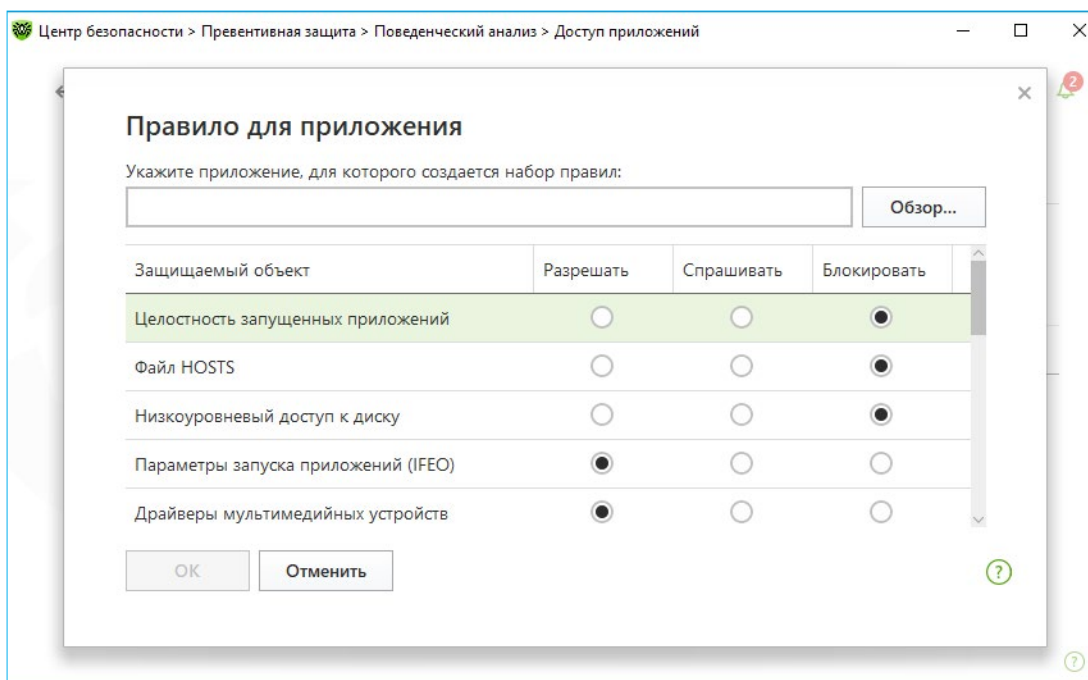
Превентивная защита Dr.Web не позволяет вредоносному ПО нарушить нормальную работу системных служб, например вмешаться в штатное создание резервных копий файлов.

Статус **Разрешать** позволяет пользователям и злоумышленникам вносить изменения в соответствующие ресурсы.

Перейдя на закладку **Доступ приложений**, вы можете задать ограничения для доступа к системе для конкретных программ, установленных у вас на компьютере.



Для этого нажмите , в открывшемся окне выберите программу и настройте ограничения для нее.



В режиме работы **Оптимальный**, установленном по умолчанию, запрещается автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему. Также запрещается низкоуровневый доступ к диску для защиты системы от заражения буткитами и троянцами-блокировщиками, которые заражают главную загрузочную запись диска. Для предотвращения


блокировки доступа к обновлениям антивируса через Интернет и блокировки доступа на сайты производителей антивирусов запрещается модификация файла HOSTS.

При повышенной опасности заражения необходимо увеличить уровень защиты до **Среднего**. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.

Внимание! В этом режиме защиты возможны конфликты совместимости со сторонним программным обеспечением, использующим защищаемые ветки реестра.

При необходимости полного контроля за доступом к критическим объектам Windows можно поднять уровень защиты до **Параноидального**. В данном случае будет доступен интерактивный контроль загрузки драйверов и автоматического запуска программ.

Чтобы самостоятельно настроить параметры работы превентивной защиты, отметьте необходимый уровень доступа к защищаемым объектам. Режим автоматически сменится на **Пользовательский**. Пользовательский режим позволяет гибко настроить реакцию антивируса на определенные действия, которые могут привести к заражению вашего компьютера.

Вы также можете, нажав , создать новый профиль и переключаться на него в случае необходимости.

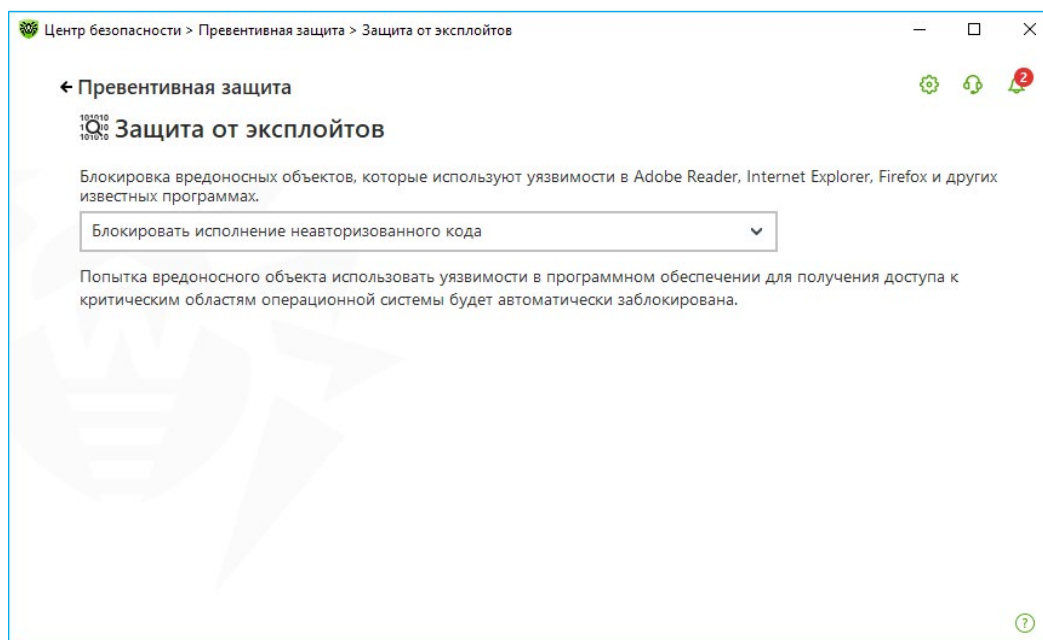
Напоминаем! Для пользователей Dr.Web [расшифровка](#) файлов, зашифрованных троянцем-вымогателем, бесплатна, если на момент инцидента были соблюдены эти [условия](#) использования Dr.Web.

Еще один компонент **Превентивной защиты** — **Защита от эксплоитов**.

Эксплоит (от англ. *exploit* — использовать, эксплуатировать) — вредоносная программа, последовательность команд или специально написанный вредоносный код, использующие уязвимости, в том числе для доставки троянцев в систему или для взлома определенного ПО. Существуют также наборы эксплоитов — «эксплоит-паки», предназначенные для использования целого ряда уязвимостей.

Эксплоит позволяет злоумышленнику внедриться в систему незаметно. Даже если ОС настроена так, что при запуске программ (одна из которых может быть и вредоносной) она выдает предупреждение о старте приложения, вредоносный код может исполниться незаметно для пользователя, благодаря эксплуатации уязвимостей.

Компонент **Защита от эксплойтов** убережет от вредоносных объектов, пытающихся для проникновения в систему использовать уязвимости в популярных приложениях, в том числе еще не известные никому, кроме вирусописателей (так называемые уязвимости нулевого дня). При обнаружении попытки проникновения через уязвимость Dr.Web принудительно завершает процесс атакуемой программы.



Это интересно! Антивирус предназначен для «ловли» вредоносных программ. Но зачастую именно внедрение вредоносного кода есть цель злоумышленников, использующих уязвимости. И если антивирус перехватывает внедряемую через даже еще никому не известную уязвимость программу — он выполняет роль защиты от уязвимостей!

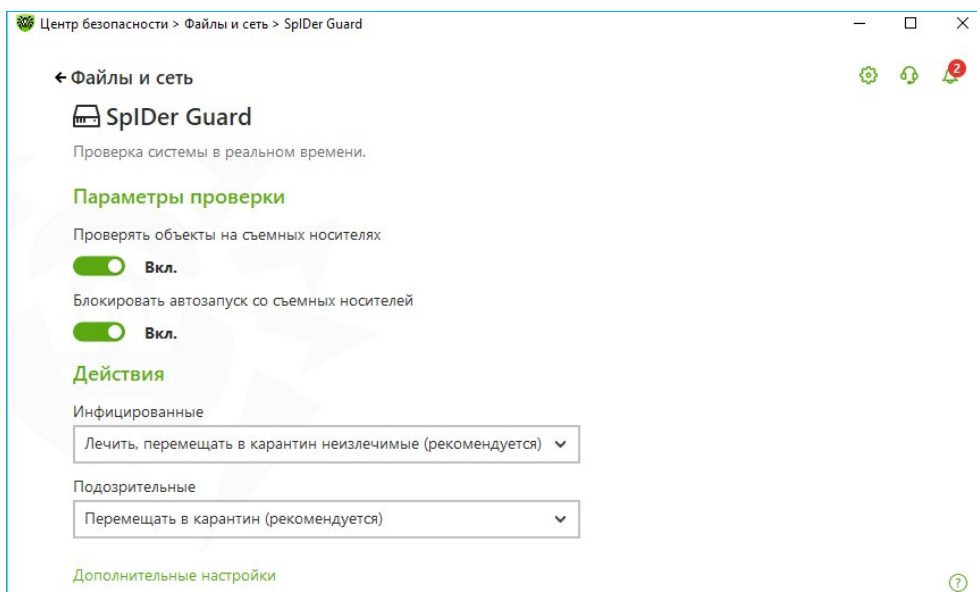
Неуязвимых систем не существует! Разработчики ПО стараются оперативно выпускать «заплаты» к известным уязвимостям. Например, компания Microsoft достаточно часто выпускает обновления безопасности. Но часть из них пользователи устанавливают с большим запозданием (или не устанавливают вовсе), что стимулирует злоумышленников как на поиск все новых уязвимостей, так и на использование уже известных, но не закрытых на стороне потенциальных жертв.

О том, как злоумышленники проникают в якобы защищенные системы, как создаются эксплойты, читайте в выпусках рубрики «[Уязвимые](#)» и «[Незванные гости](#)» проекта «Антивирусная правДА!».

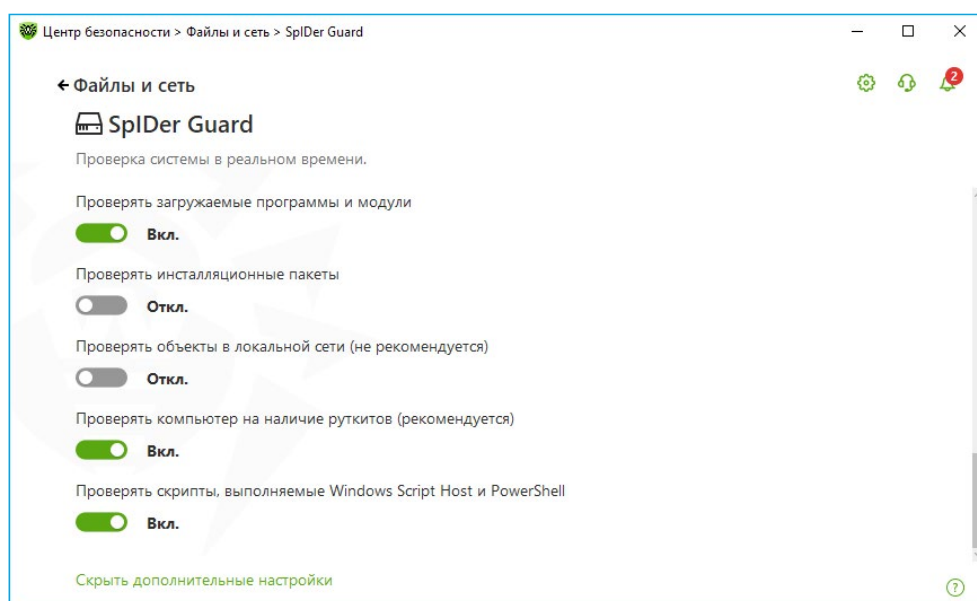
Также обнаружение ранее не известных вредоносных программ обеспечивается модулем фоновой проверки запущенных процессов и нейтрализации активных

угроз, а также проведением периодической антивирусной проверки. Данная подсистема реализована в рамках Антируткита Dr.Web. Подсистема постоянно находится в памяти и осуществляет поиск активных угроз в следующих критических областях Windows: объекты автозагрузки, запущенные процессы и модули, эвристики системных объектов, оперативная память, MBR/VBR дисков, системный BIOS компьютера. При обнаружении угроз данная подсистема может оповещать пользователя об опасности, осуществлять лечение и блокировать опасные действия.

Для включения режима проверки на руткиты в окне **Центр безопасности** выберите **Файлы и сеть** и далее **SplDer Guard**. Нажмите на **Дополнительные настройки**.





Прокрутите бегунок справа до появления строки **Проверить компьютер на наличие руткитов**.

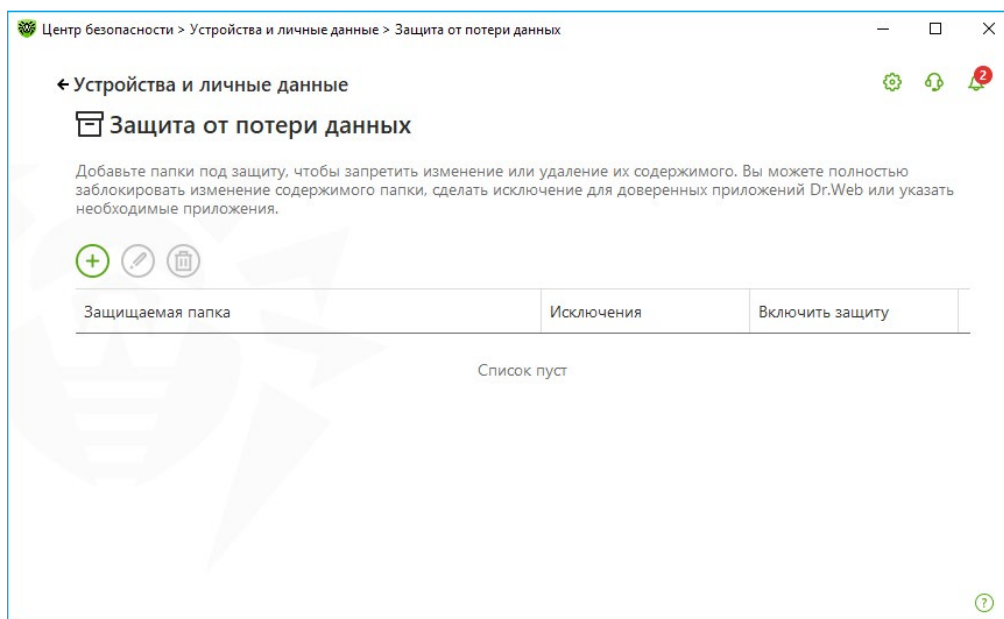



Данный параметр включен по умолчанию.

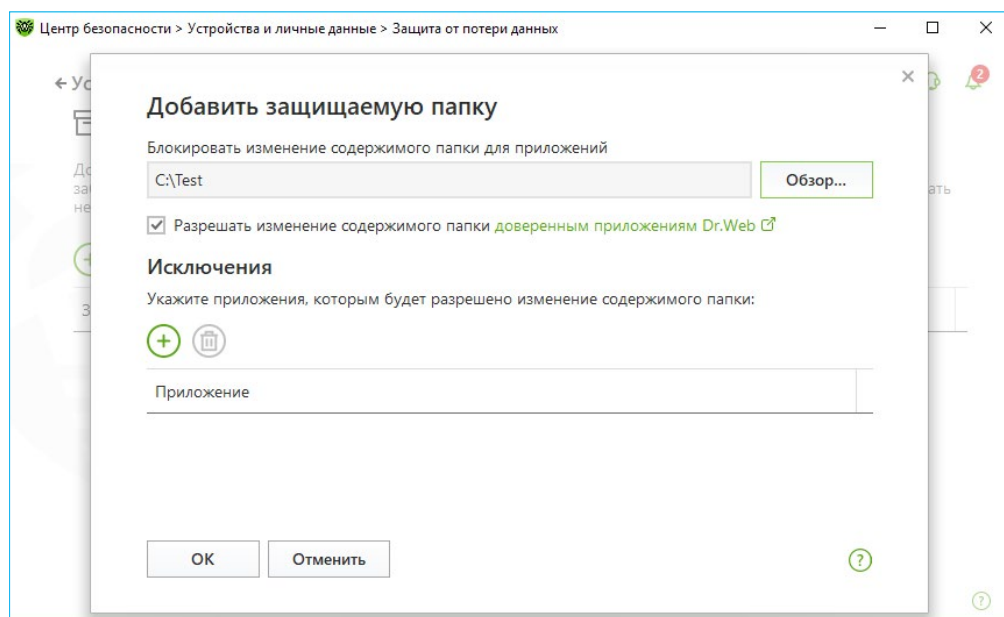
2.7. Функционал «Защита от потери данных»


Для настройки параметров «Защиты от потери данных» кликните на значок  в системном меню, затем в открывшемся меню агента нажмите на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).

В окне **Центр безопасности** выберите **Устройства и личные данные** и далее **Защита от потери данных**.



В открывшемся окне нажмите  и сформируйте список папок, помещенных под защиту.





В том случае, если вы хотите вручную сформировать список программ, имеющих доступ к защищаемым данным, — нажмите  и укажите имена программ, которым вы даете такое право.

2.8. Ограничение возможности проникновения шифровальщиков на компьютер

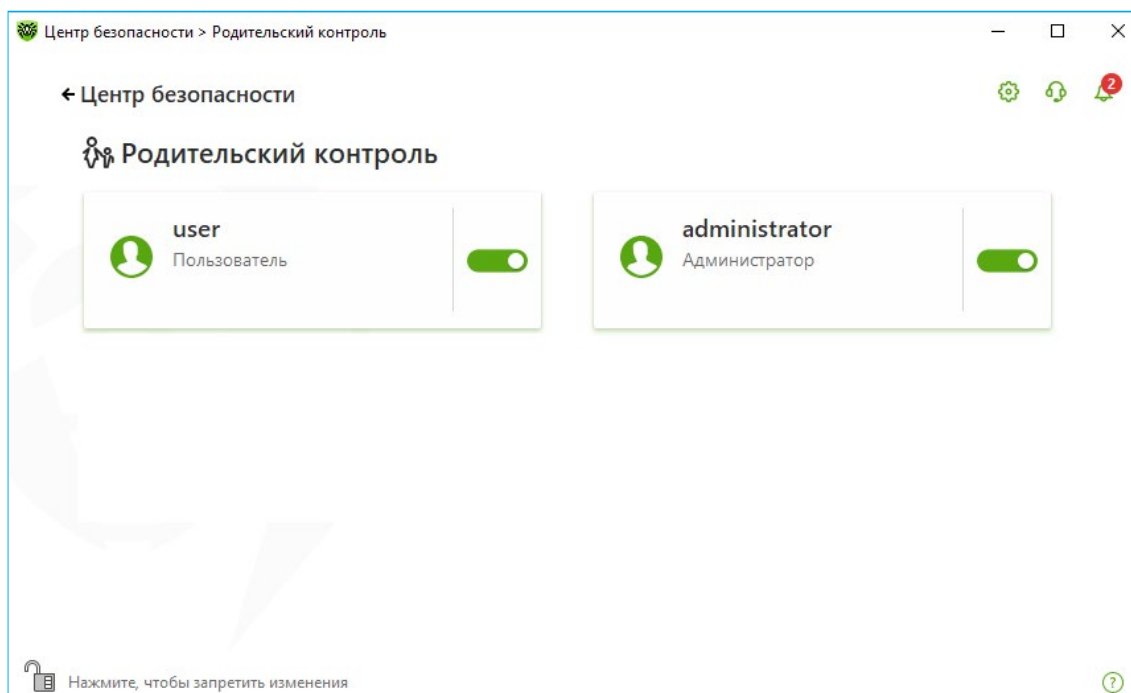
2.8.1. Использование Офисного/Родительского контроля

Троянец-шифровальщик может проникнуть в локальную сеть или на отдельный компьютер через спам (как правило, сообщение содержит вредоносное вложение или специально сформированную ссылку), с помощью сообщения мессенджера (также содержащего ссылку), путем загрузки пользователем с зараженного сайта или на зараженной флешке. Для снижения риска заражения необходимо использовать антиспам, а также ограничить возможность работы с потенциально опасными интернет-ресурсами и сменными носителями.

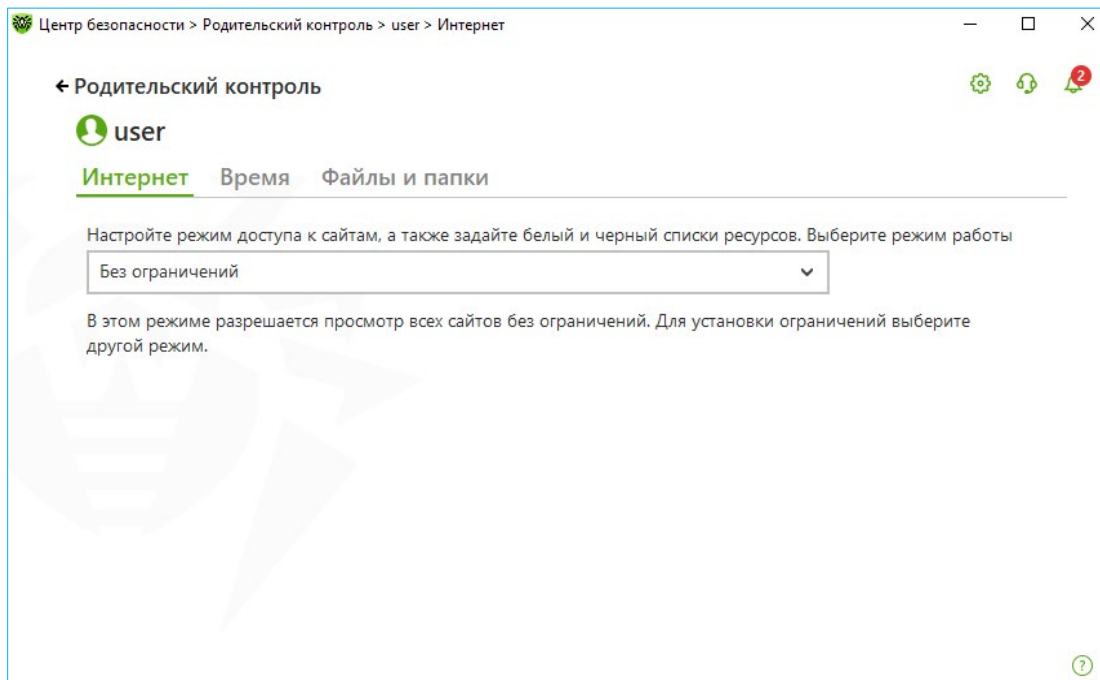
Настройка Антиспама Dr.Web не рассматривается в этом курсе, т. к. этот модуль начинает действовать по умолчанию с момента установки Dr.Web Security Space и не требует дополнительной настройки.

Для настройки режима доступа к интернет-ресурсам, а также ограничения доступа к файлам и папкам, последовательно кликните на значок  в системном меню, затем в открывшемся меню агента на кнопку **Центр безопасности** и в открывшемся окне нажмите на  (Режим администратора).

В окне **Центр безопасности** выберите **Родительский контроль**.

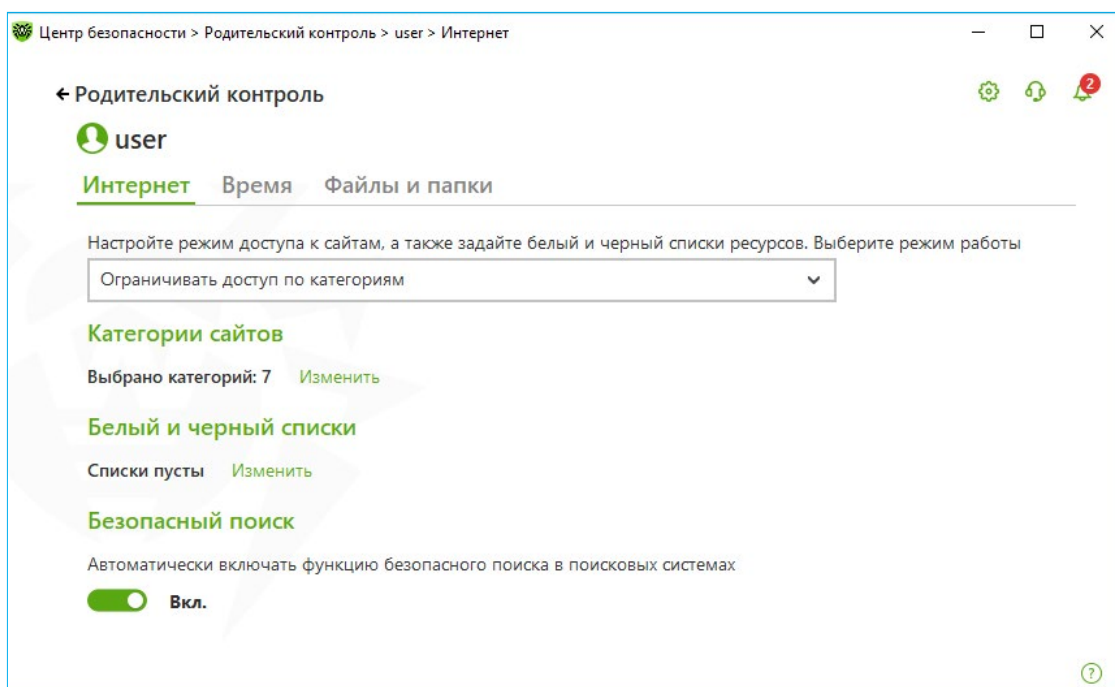


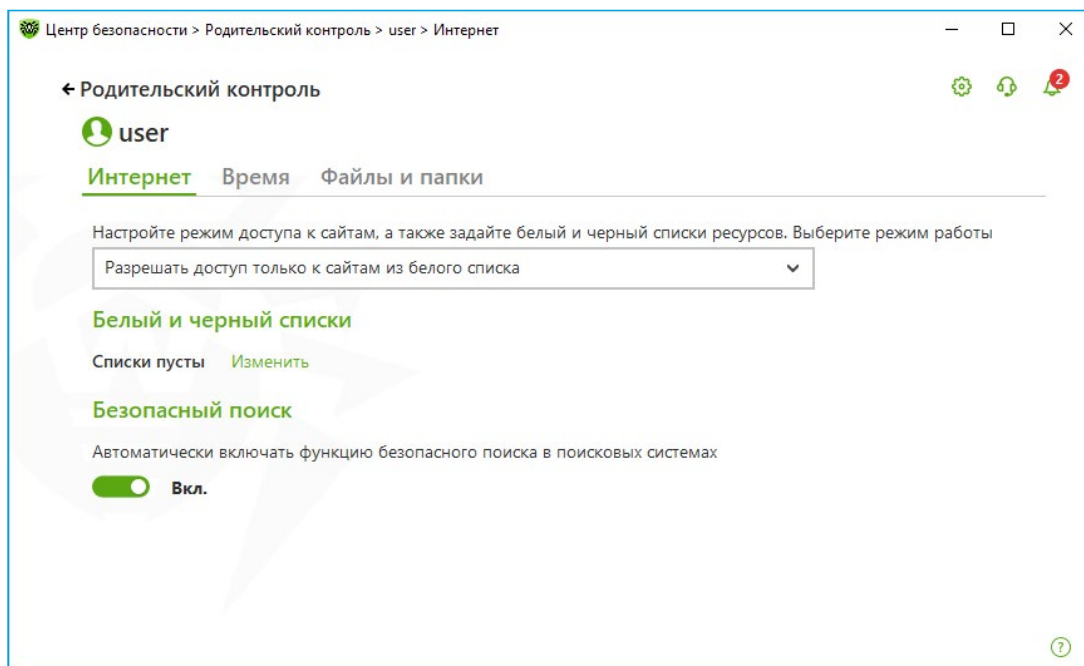
В открывшемся окне выберите пользователя, для которого необходимо настроить ограничения и сделать необходимые настройки.



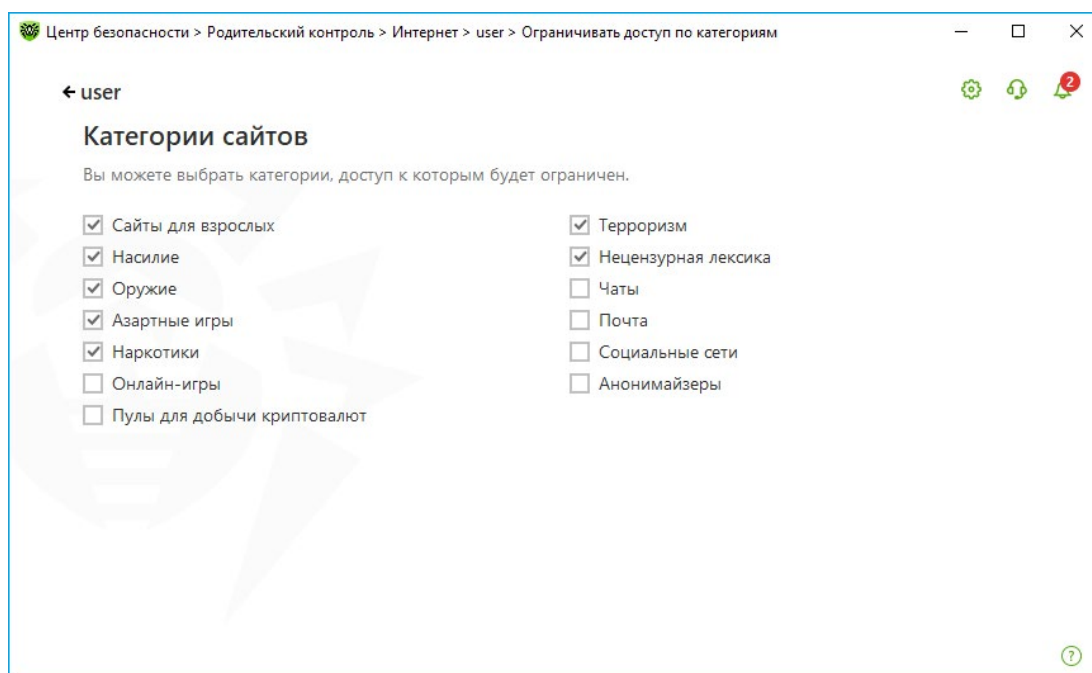
По умолчанию ограничения отключены.

Выберите вкладку **Интернет** для настройки правил доступа к интернет-ресурсам. Здесь можно запретить доступ к сайтам, посвященным насилию, азартным играм и т. п., а также разрешить посещение указанных сайтов. Рекомендуется использовать режимы **Ограничить доступ по категориям** или **Разрешать доступ только к сайтам из белого списка**.



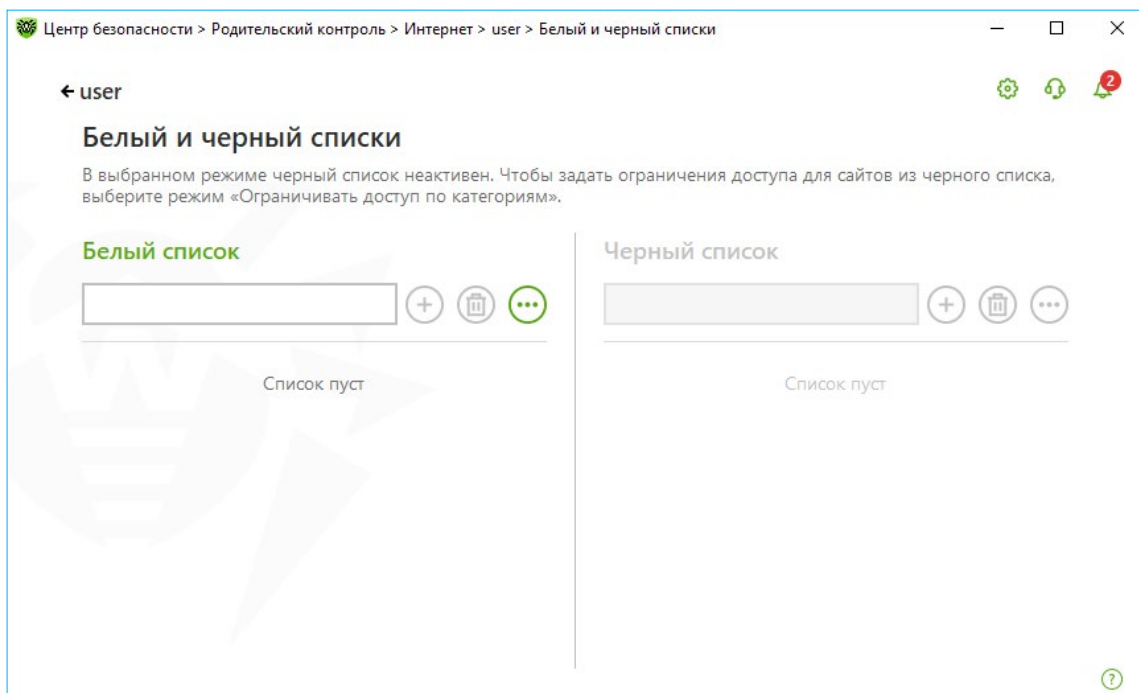



Выбрав режим **Ограничить доступ по категориям** и кликнув на **Изменить**, выберите категории ресурсов, доступ к которым нужно блокировать.



Отметьте необходимые категории, доступ к которым нужно запретить.

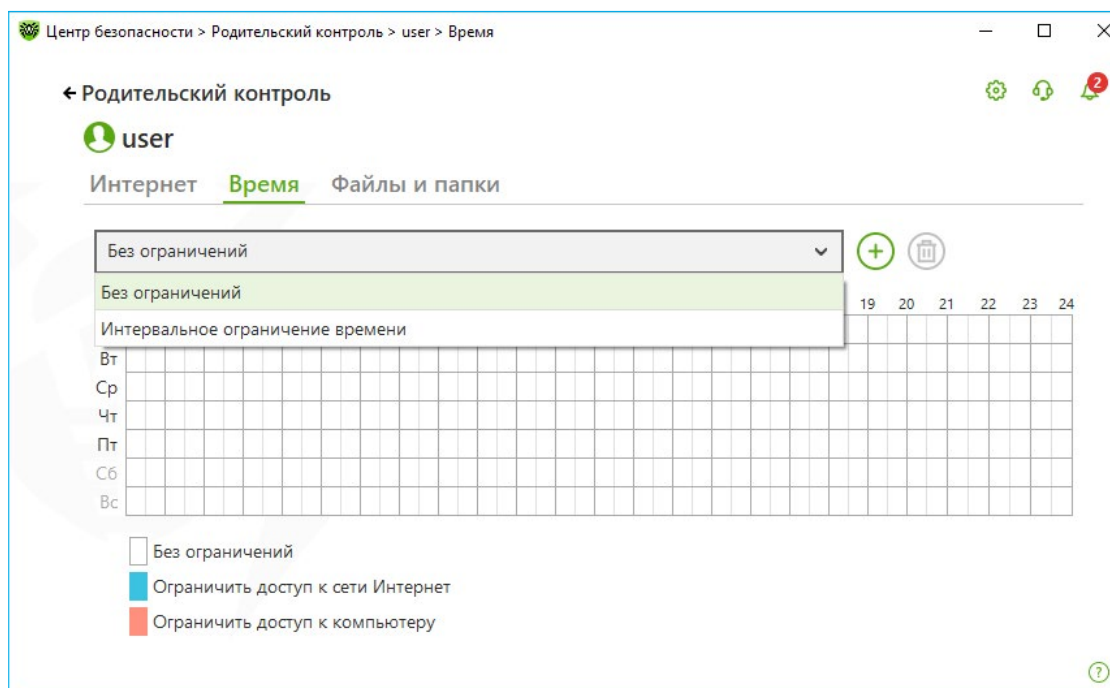
В обоих рекомендуемых режимах вы можете настроить белые и черные списки доступа к ресурсам, нажав на кнопку **Изменить** в группе настроек **Белый и черный списки**.




Для добавления ресурса нажмите  для соответствующего списка. Для обоих списков можно использовать доменные имена ресурсов или части доменных имен, а также маски.

Опция **Безопасный поиск** позволяет исключить нежелательные ресурсы из результатов поиска, используя средства поисковых систем.

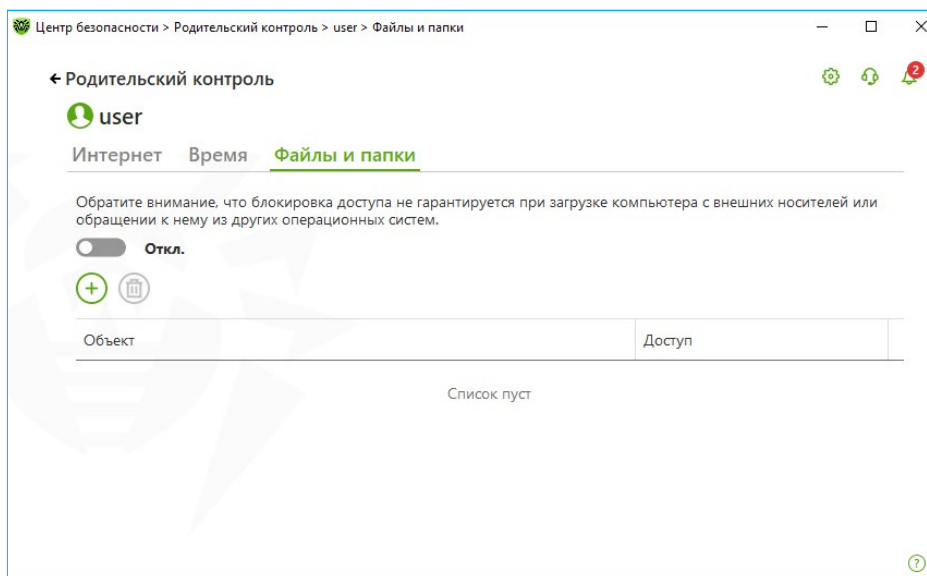
На вкладке **Время** вы можете ограничить время работы пользователей за компьютером и в Интернете. Данная возможность позволяет исключить неконтролируемый доступ к ресурсу в неразрешенное время.




Нажав , вы можете создать профиль настроек. В профиле сохранятся настоящие настройки таблицы. В дальнейшем при изменении настроек профиля они будут также автоматически сохраняться.

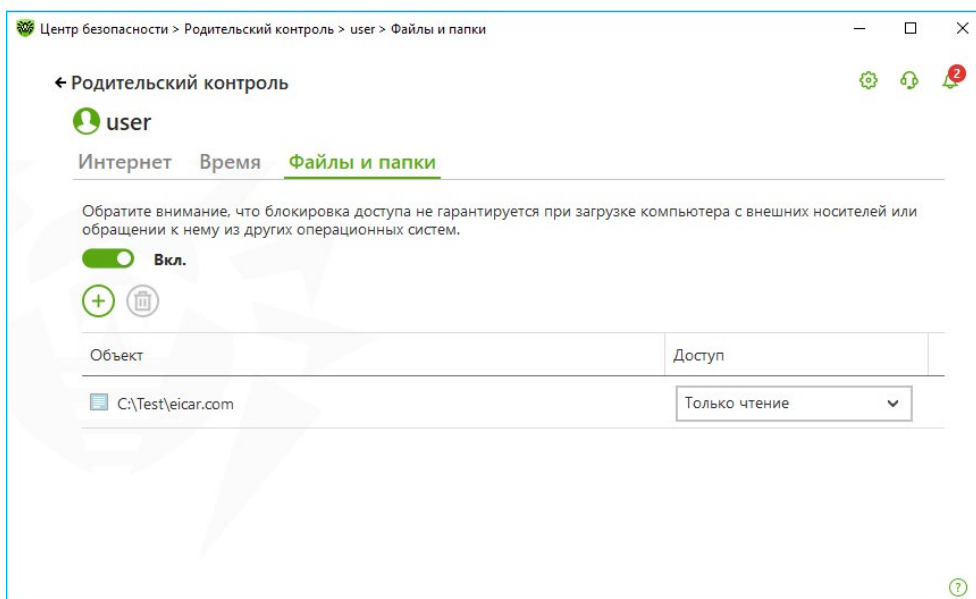
На вкладке **Файлы и папки** ограничьте доступ к файлам и папкам на локальных дисках и на съемных носителях.

Включите ограничение доступа к файлам и папкам, передвинув переключатель.



Внимание! Ограничение доступа не гарантируется при загрузке компьютера со съемных носителей или обращении к заданным объектам из других операционных систем, установленных на компьютере.

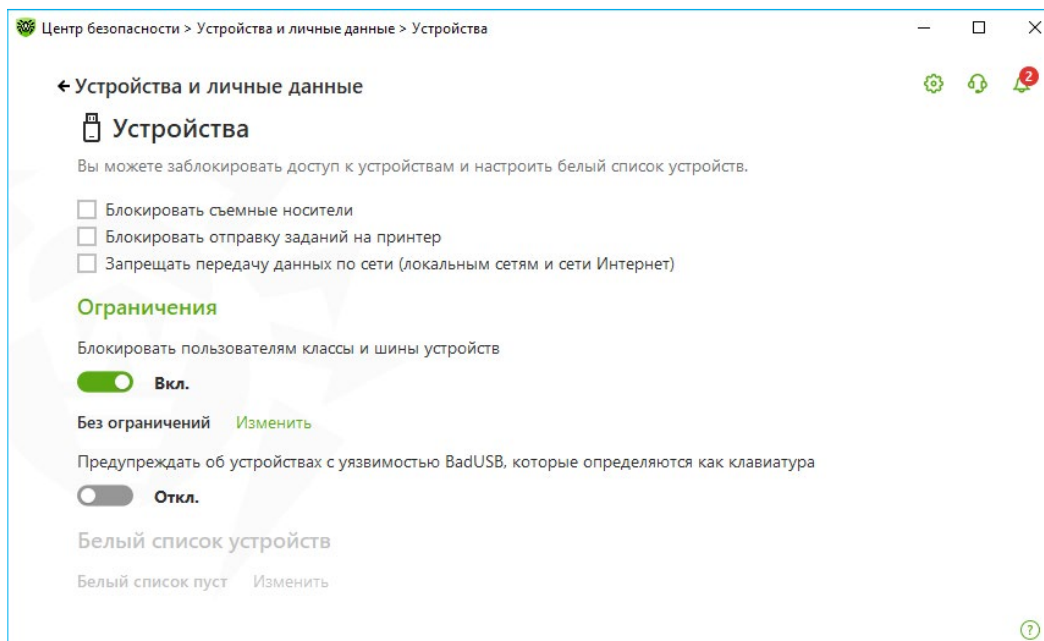
Нажав , добавьте необходимые папки и файлы в список ресурсов, доступ к которым будет ограничен.



Выберите режим доступа для добавленного объекта:

- **Заблокирован** — для полной блокировки доступа к объекту.
- **Только чтение** — для того, чтобы разрешить доступ к объекту без его изменения, удаления или перемещения (например, просмотр документа, изображения, запуск исполняемого файла).

Для настройки ограничений действий со сменными носителями в окне **Центр безопасности** выберите **Устройства и личные данные** и далее **Устройства**.

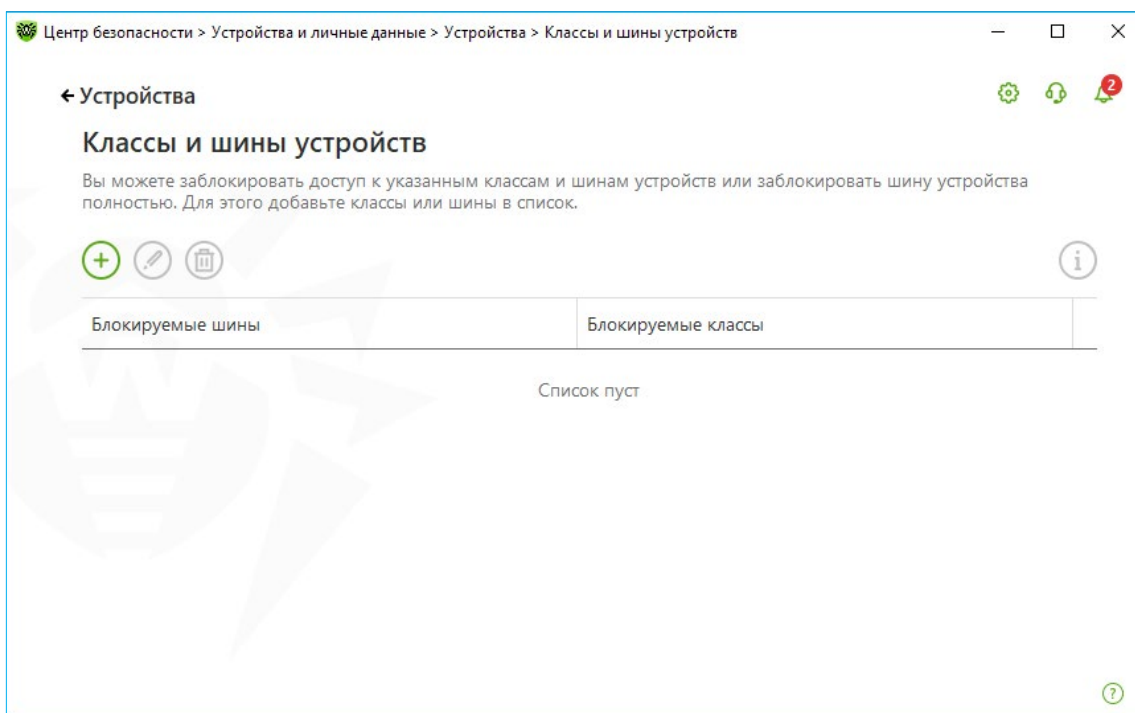


В данном окне вы можете полностью заблокировать доступ к данным на съемных носителях (USB флеш-накопителях, дискетах, CD/DVD приводах, ZIP-дисках и т. п.), выбрав **Блокировать съемные носители**.

Если вы хотите заблокировать доступ к отдельным устройствам и типам устройств, передвиньте переключатель **Блокировать указанные устройства для всех пользователей**, нажмите кнопку **Изменить** и в открывшемся окне составьте список классов и шин устройств, доступ к которым хотите заблокировать.

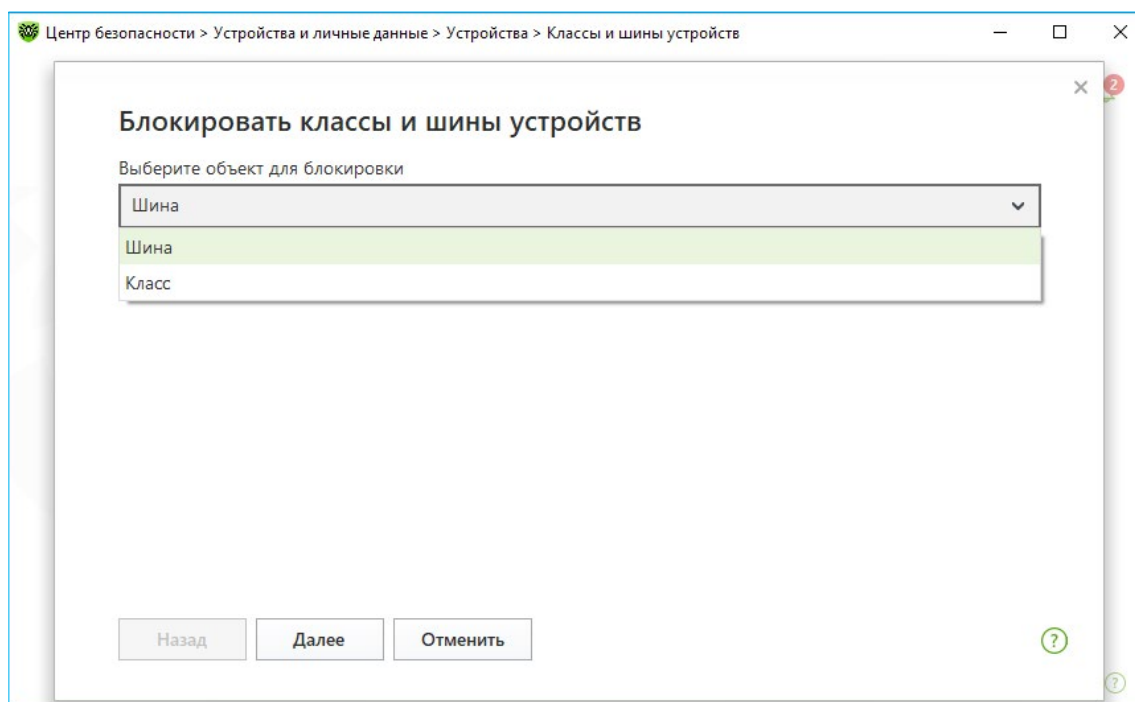
Класс устройства — специальный код, передаваемый устройством операционной системе, позволяющий операционной системе выбрать правильный драйвер и определить перечень функционала, предоставляемый устройством (аудиоустройства ввода/вывода, биометрические устройства, дисковые устройства, DVD/CD-ROM, дисководы, устройства GPS, камеры/фотоаппараты, инфракрасные устройства, клавиатуры, мыши и иные подобные устройства, модемы, сетевые карты, принтеры и т. д.).

Шина устройства — способ подключения к компьютеру (Bluetooth, IEEE 1394, USB, последовательный/параллельный порт, устройства чтения смарт-карт, PCMCIA, шина PCI и т. д.).

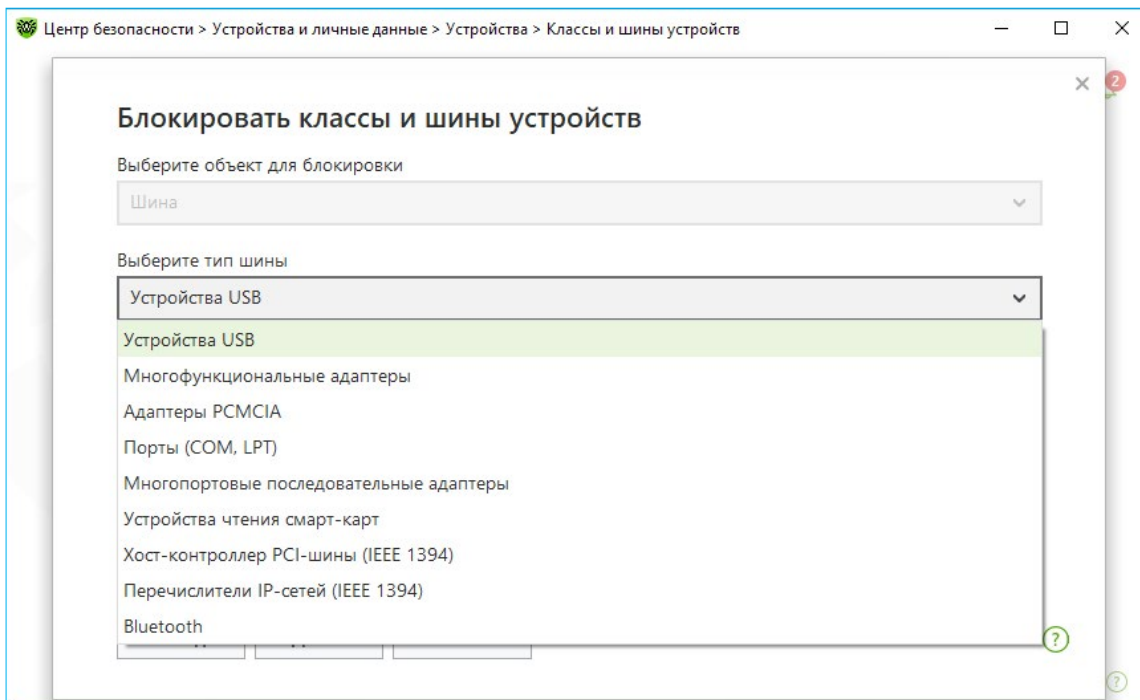


Для добавления шины полностью или некоторого устройства на определенной шине в список используйте **+**.

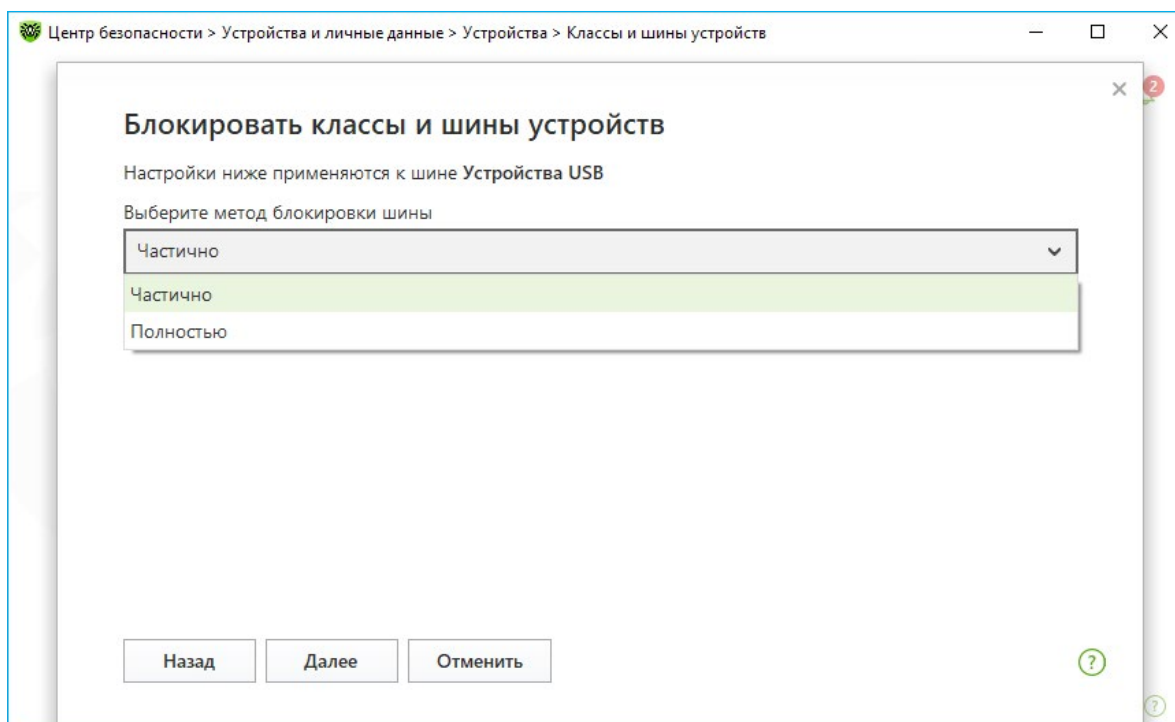
Если вы хотите заблокировать шину, то из выпадающего списка выберите **Шина** и нажмите **Далее**.



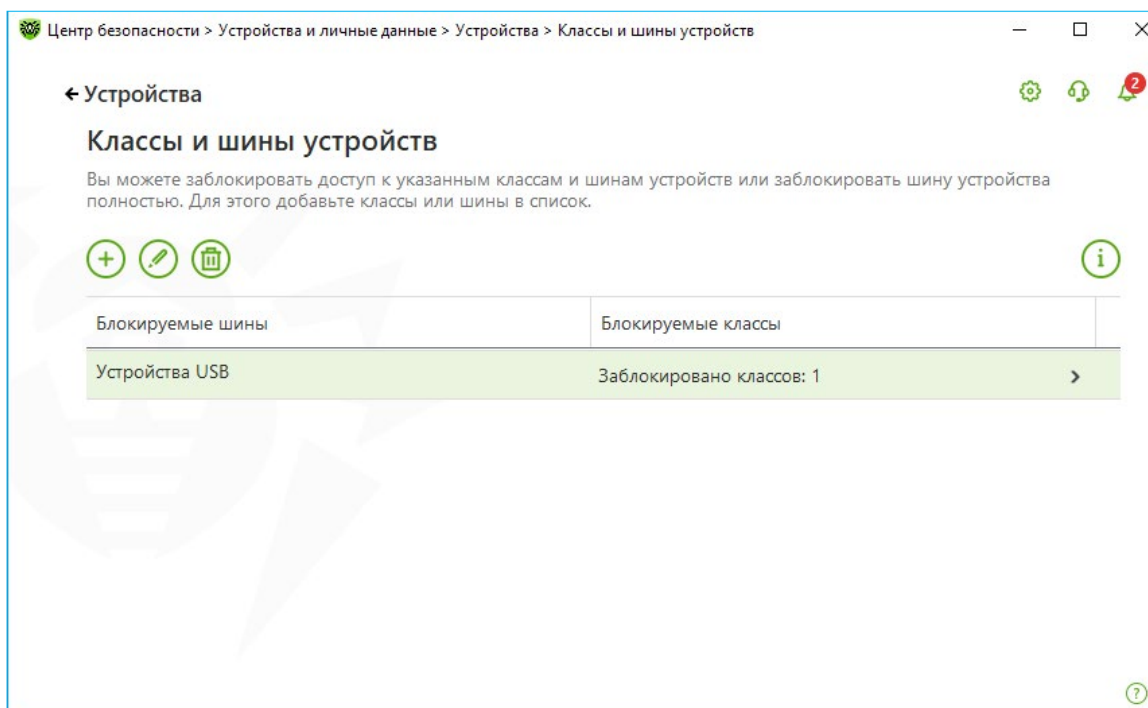
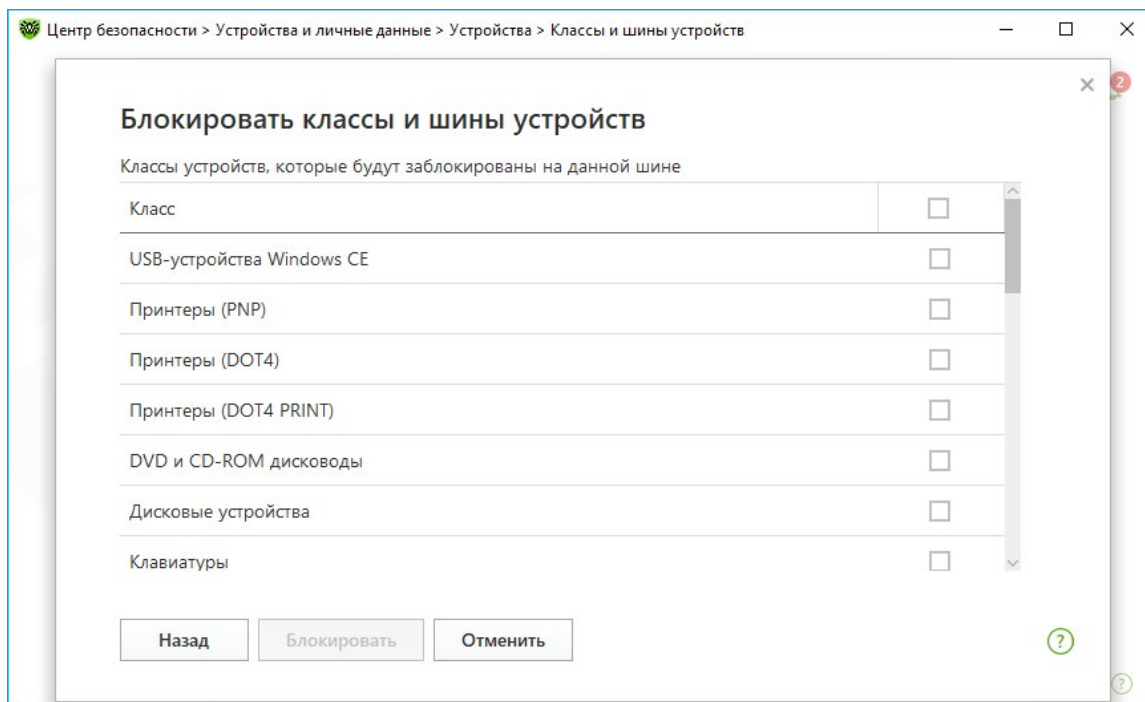
Выберите тип шины.



Выберите тип блокировки (**Полностью** — будут заблокированы все классы устройств на данной шине или **Частично** — откроется окно выбора классов устройств для блокировки на данной шине) и нажмите **Далее**.

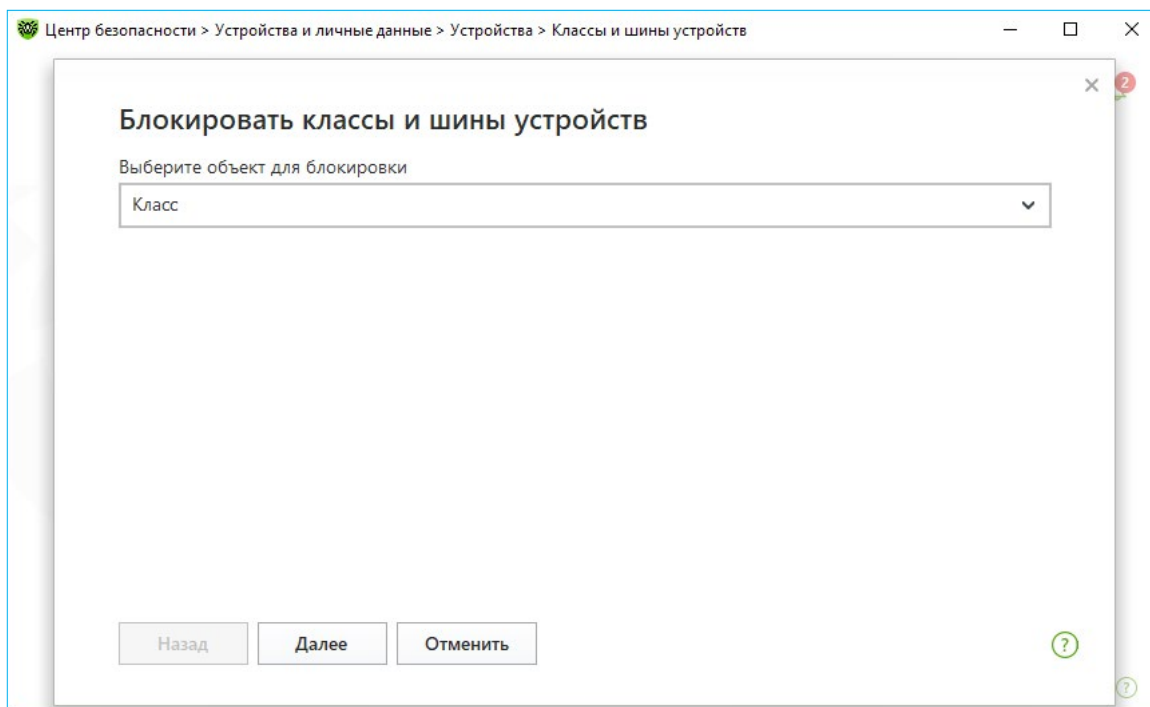


Отметьте классы из списка, которые вы хотите заблокировать. Нажмите **Блокировать**.

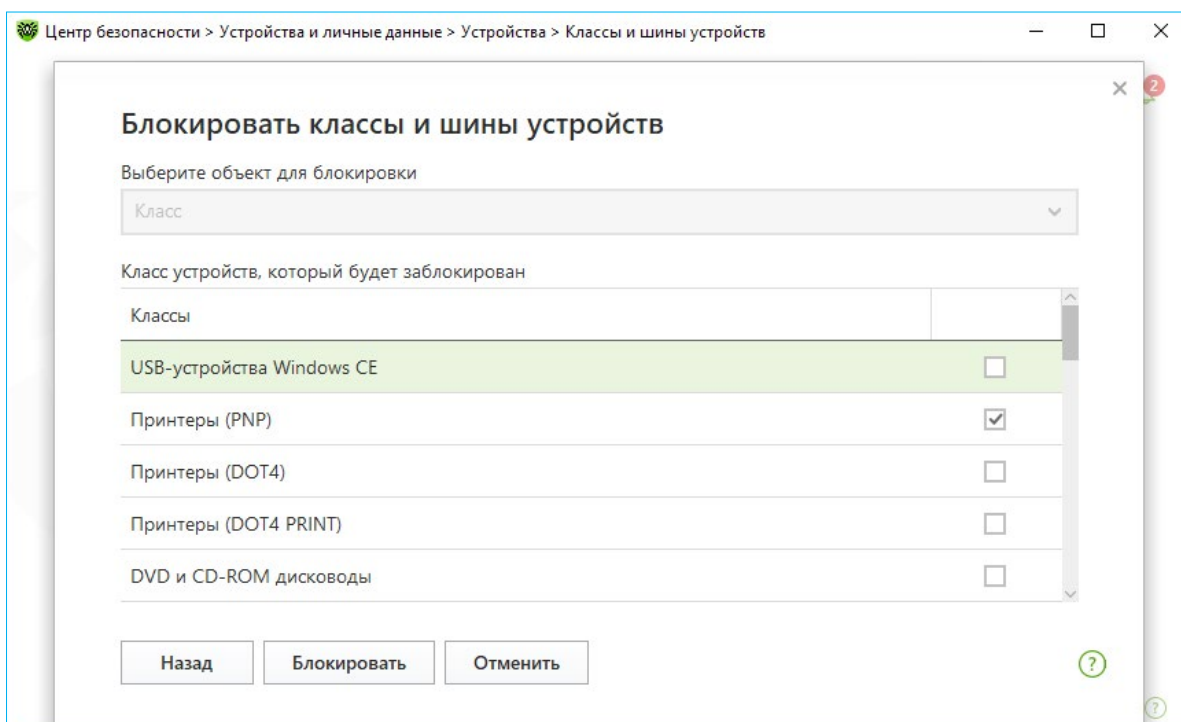


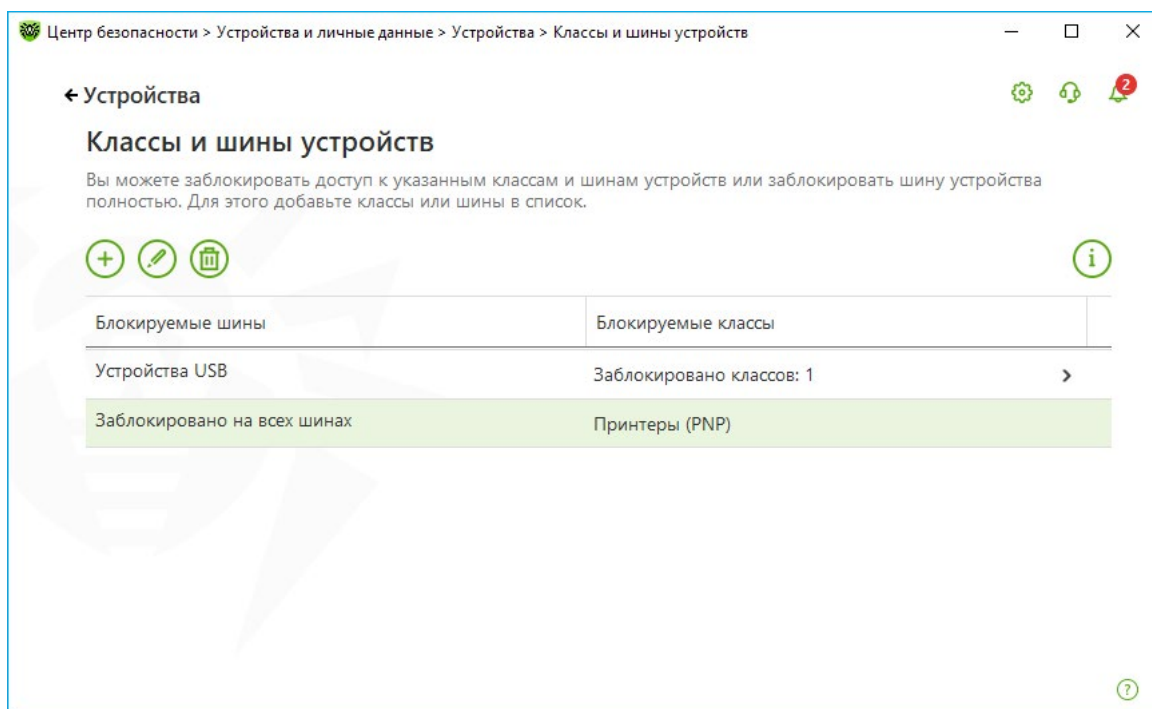
Внимание! При блокировке шины USB клавиатура и мышь вносятся в исключения.

Чтобы заблокировать один или несколько классов устройств, нажмите кнопку . В открывшемся окне из выпадающего списка выберите **Класс** и нажмите **Далее**.



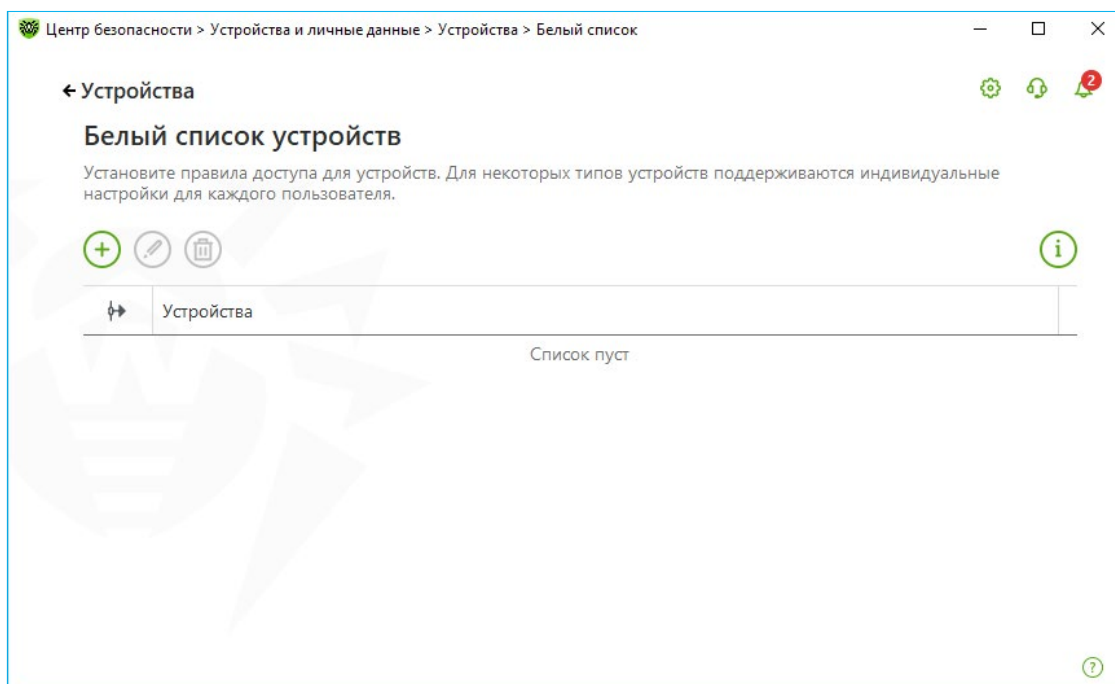
Отметьте те классы из списка, которые вы хотите заблокировать. Нажмите **Блокировать**.





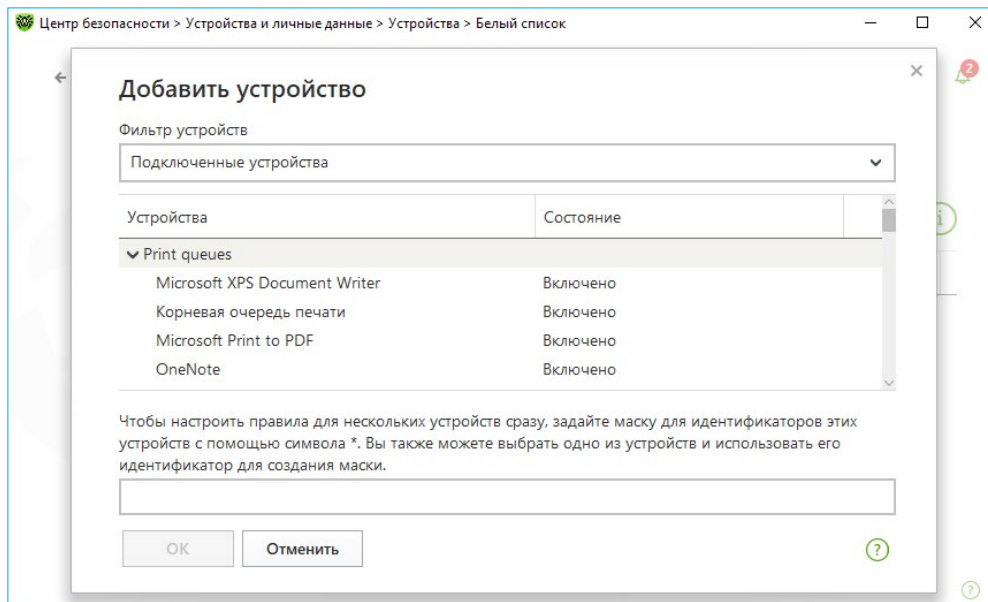
Внимание! При активации блокировки уже подключенного устройства требуется либо подключить устройство заново, либо перезагрузить компьютер. Блокировка работает только для устройств, подключенных после активации функции.

Для формирования белого списка устройств в группе настроек **Белый список** устройств нажмите кнопку **Изменить**.

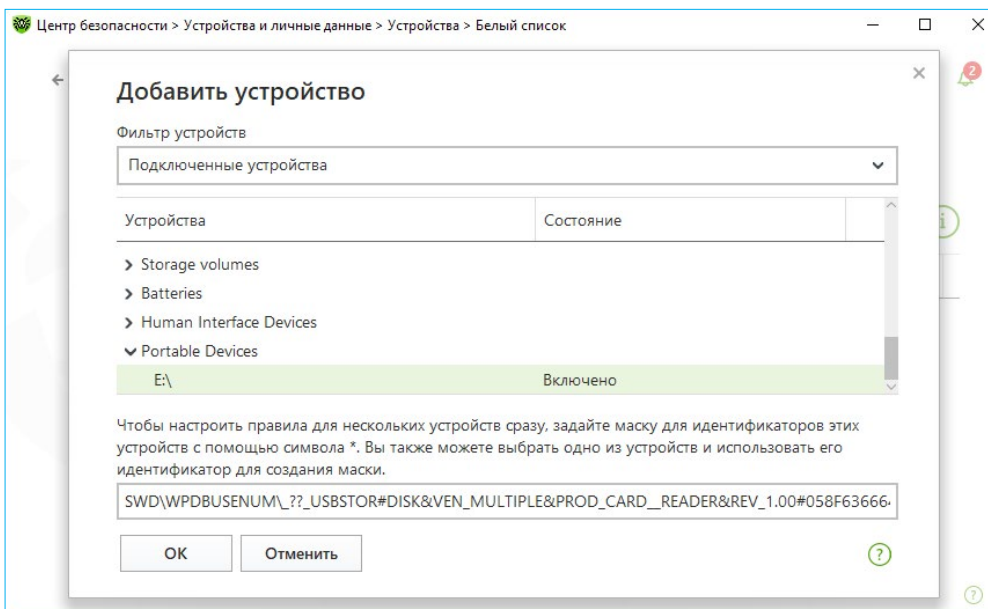


Окно **Белый список устройств** содержит информацию обо всех устройствах, добавленных в белый список.

Для добавления устройства в белый список подключите его к компьютеру и нажмите **+**.



В открывшемся окне нажмите кнопку **Обзор** и выберите нужное устройство. В выпадающем списке выберите показ только подключенных или только отключенных устройств.

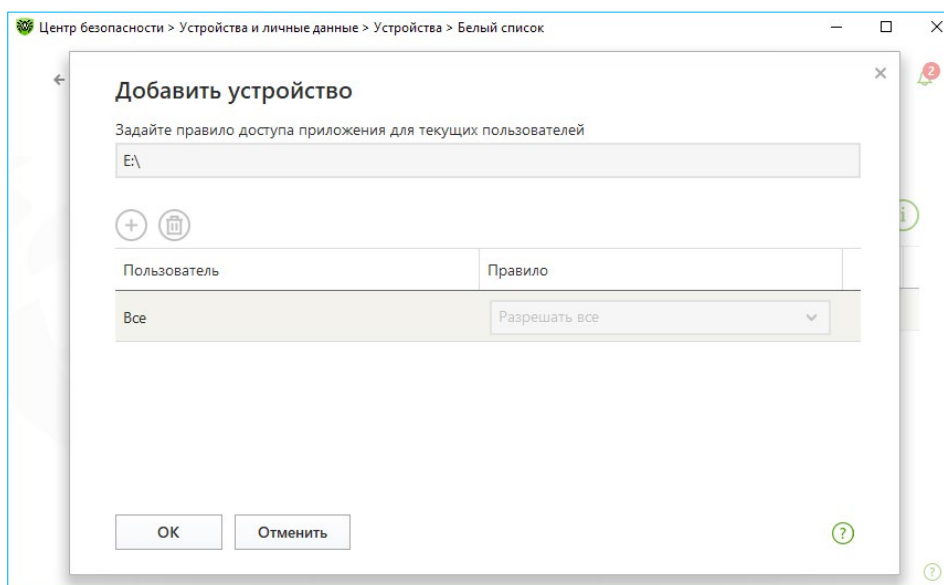
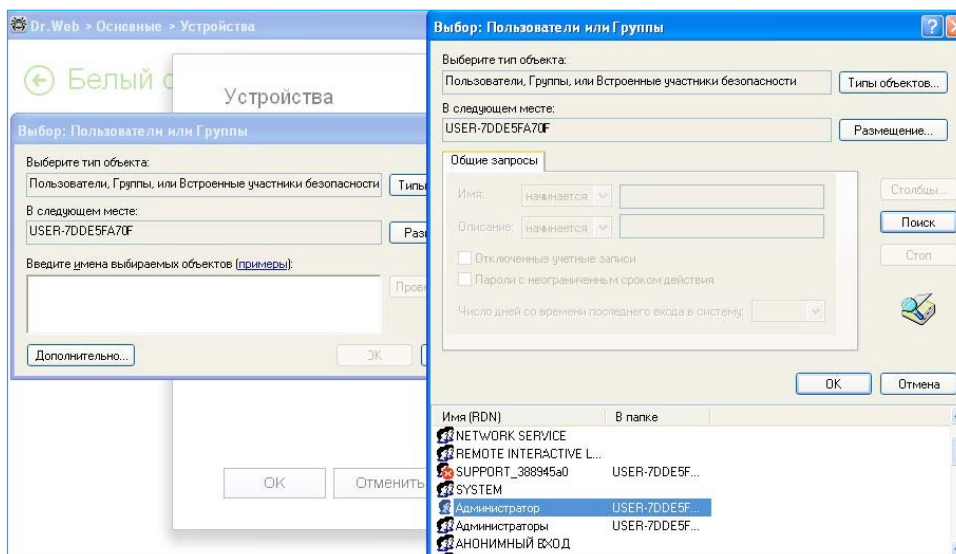


Нажмите кнопку **OK**.

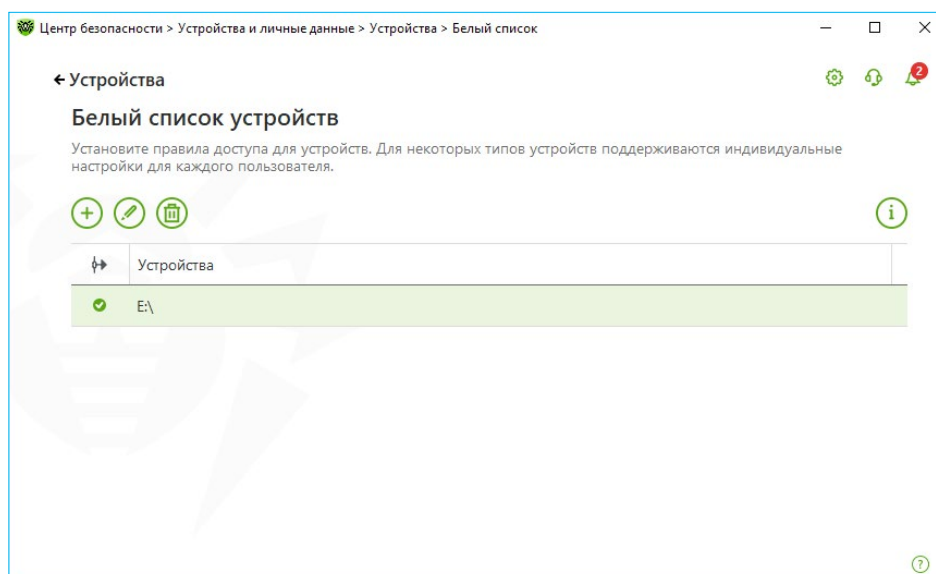
Для устройств с файловой системой вы можете настроить правила доступа.

Для этого в столбце **Правило** выберите один из режимов: **Разрешать все** или **Только чтение**. Чтобы добавить новое правило для конкретного

пользователя, нажмите **+**, **Поиск** и выберите необходимого пользователя.



Нажмите кнопку **ОК**.



2.8.2. Использование Брандмауэра

- Непонятно как произошло заражение, так как не открывались незнакомые сообщения.*
- Как произошло заражение не знаю, включила ноутбук, файлы зашифрованы.*
- Заражение прошло внезапно, до этого машина использовалась как телевизор, ничего не скачивалось и не устанавливалось.*

Обращения в техническую поддержку

* Пользователь не использовал продукты Dr.Web.



Иногда для заражения компьютера не требуется открывать письмо или кликать по ссылке — достаточно не устанавливать обновления и открыть доступ к компьютеру со стороны Интернета.

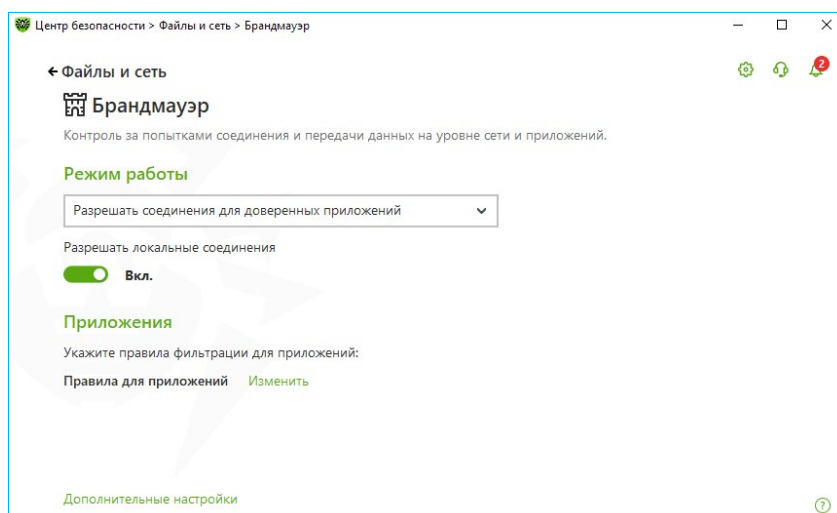
Брандмауэр необходим для защиты от несанкционированного доступа извне и предотвращения утечки важных данных по сети.

Чтобы сетевой червь-шифровальщик WannaCry проник на компьютер, необходимо несколько условий:

1. Отсутствуют обновления безопасности (такое бывает, если система автоматического обновления отключена, пользователь отказался от установки обновлений или используется неподдерживаемая производителем операционная система).
2. Открыты интересующие злоумышленника сетевые порты. В частности, порт 445.
3. Разрешен сервис SMB v1.

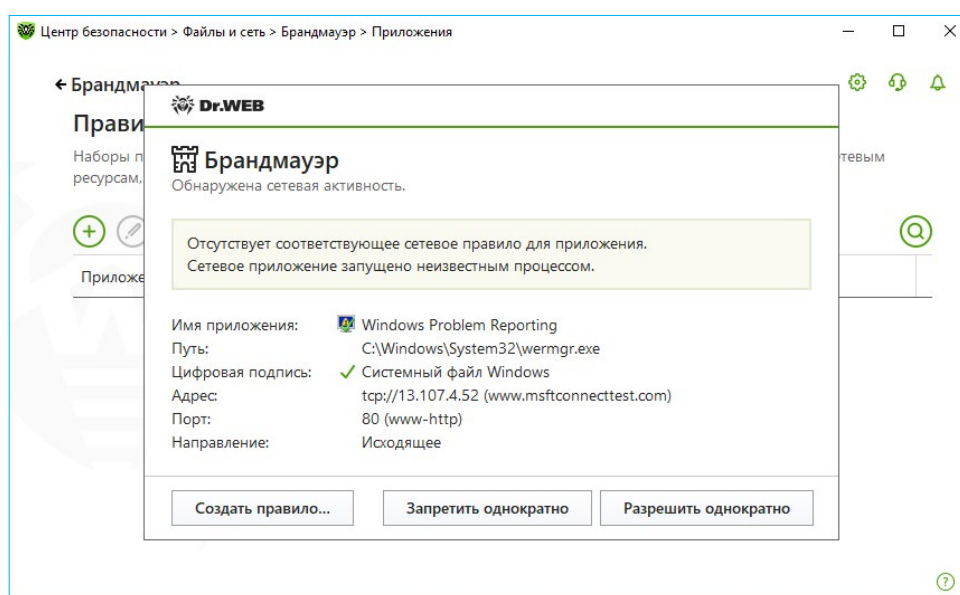
Невыполнение хотя бы одного из этих условий приводит к тому, что сетевой червь не сможет проникнуть на компьютер.

Для настройки параметров работы Брандмауэра щелкните кнопкой мыши по значку  в системном меню, затем в открывшемся меню агента на кнопку Центр безопасности и в открывшемся окне нажмите на  (Режим администратора). В окне **Центр безопасности** выберите **Файлы и сеть** и далее **Брандмауэр**.



Выберите один из следующих режимов работы:

- **Разрешать неизвестные соединения** — режим, при котором всем неизвестным приложениям предоставляется доступ к сетевым ресурсам;
- **Разрешать соединения для доверенных приложений** — режим, при котором всем доверенным приложениям предоставляется доступ к сетевым ресурсам (используется по умолчанию), для всех остальных приложений выдается предупреждение, где вы можете задать правило;
- **Интерактивный режим** — режим, в котором при обнаружении попытки системы или приложений подключиться к сети Брандмауэр проверяет, заданы ли для этих программ правила фильтрации. Если правила отсутствуют, то выводится соответствующее предупреждение, где вы можете задать правило.



Внимание! При работе под учетной записью с ограниченными правами (Гость) Брандмауэр Dr.Web не выдает пользователю предупреждения о попытках доступа к сети. Предупреждения будут выдаваться под учетной записью с правами администратора, если такая сессия активна одновременно с гостевой.

Внимание! В некоторых случаях операционная система Windows не позволяет однозначно идентифицировать службу, работающую как системный процесс. При обнаружении попытки подключения со стороны системного процесса обратите внимание на порт, указанный в сведениях о соединении. Если вы используете приложение, которое может обращаться к указанному порту, разрешите данное подключение.

В случаях когда программа, осуществляющая попытку подключения, уже известна Брандмауэру (то есть для нее заданы правила фильтрации), но запускается другим неизвестным приложением (родительским процессом), Брандмауэр выводит соответствующее предупреждение.

Правила для родительских процессов

1. При обнаружении попытки подключения к сети со стороны приложения, запущенного иным (родительским) приложением — неизвестным для Брандмауэра, ознакомьтесь с информацией об исполняемом файле этой родительской программы.

2. Когда вы примете решение о подходящей для данного случая операции, выполните одно из следующих действий:

- чтобы однократно заблокировать подключение приложения к сети, нажмите кнопку **Запретить**;
- чтобы однократно позволить приложению подключиться к сети, нажмите кнопку **Разрешить**;
- чтобы создать правило, нажмите **Создать правило** и в открывшемся окне задайте необходимые настройки для родительского процесса.

3. Нажмите кнопку **ОК**. Брандмауэр выполнит указанную вами операцию, и окно оповещения будет закрыто.

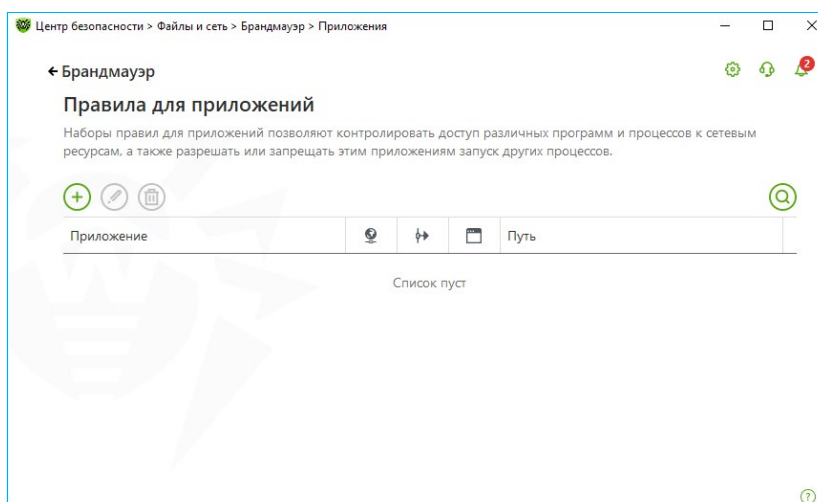
Также возможна ситуация, при которой неизвестное приложение запускается другим неизвестным приложением. В таком случае в предупреждении будет выведена соответствующая информация, и при выборе **Создать правило** откроется окно, в котором вы можете настроить правила как для приложений, так и для родительских процессов.

- **Блокировать неизвестные соединения** — режим, при котором все неизвестные подключения автоматически блокируются. Известные соединения обрабатываются Брандмауэром согласно заданным правилам фильтрации.

2.8.2.1. Ограничение прав сетевых приложений

С помощью Брандмауэра можно ограничить доступ приложений в Интернет. Фильтрация на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам.


Для ограничения доступа приложения к сетевым ресурсам, а также запрета для них запуска других сетевых приложений в разделе настроек **Приложения** нажмите **Изменить**.

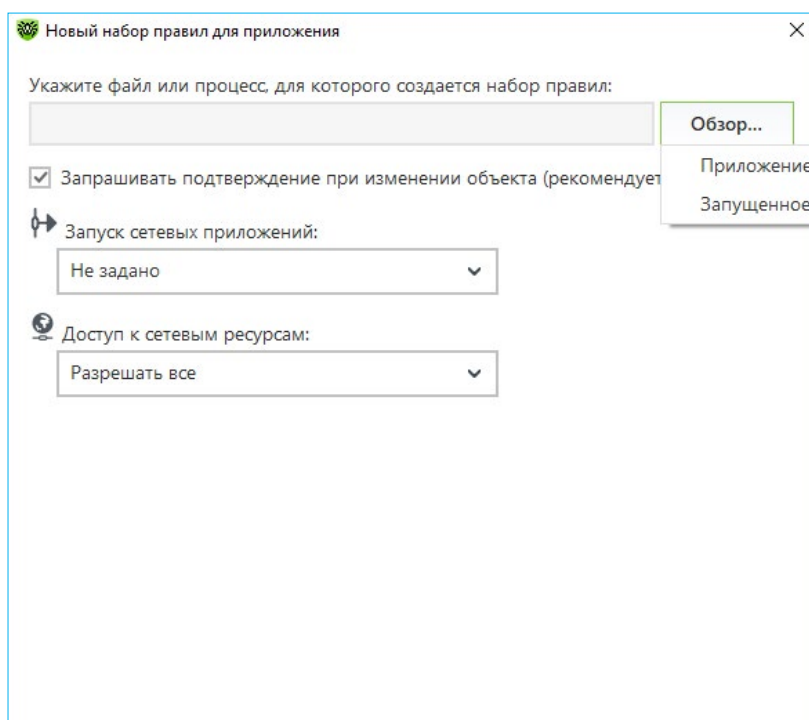


Внимание! Для каждой программы может быть не более одного набора правил фильтрации.

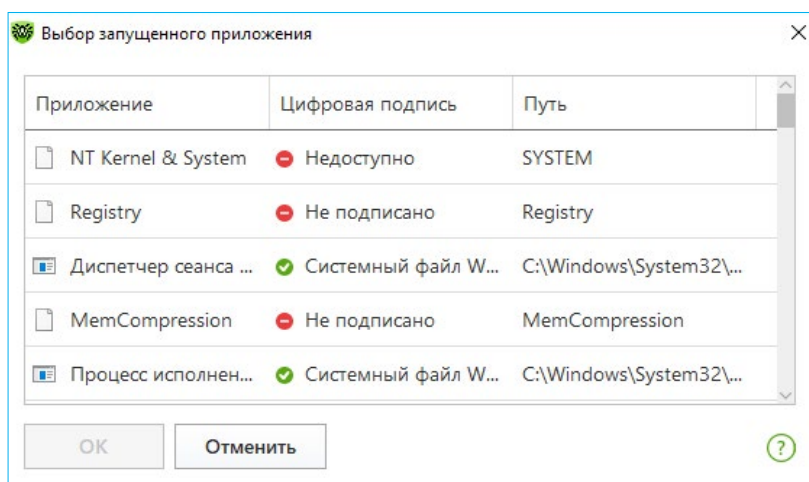
Если вы создали блокирующее правило для процесса или установили режим **Блокировать неизвестные соединения**, а потом отключили блокирующее правило или изменили режим работы, блокировка будет действовать до повторной попытки установить соединение после перезапуска процесса.



Для формирования набора правил выполните одно из следующих действий:

- Чтобы создать набор правил, нажмите на кнопку  (Создать).



Нажав **Обзор**, вы можете выбрать два варианта поиска приложения по месту размещения на диске и среди запущенных приложений.



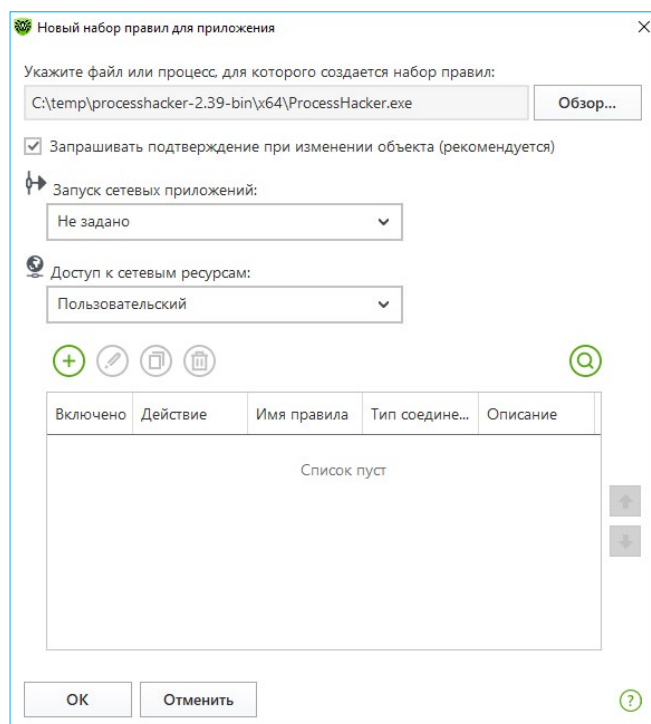
- Чтобы отредактировать существующий набор правил, выберите его в списке и нажмите на кнопку  (Изменить).
- Чтобы добавить копию существующего набора правил, выберите **Копировать** в контекстном меню. Копия добавляется под выбранным набором.
- Чтобы удалить все правила для программы, выберите соответствующий набор в списке и нажмите на кнопку  (Удалить)

При работе Брандмауэра в **Интерактивном** режиме, вы можете инициировать создание правила непосредственно из окна оповещения о попытке несанкционированного подключения.

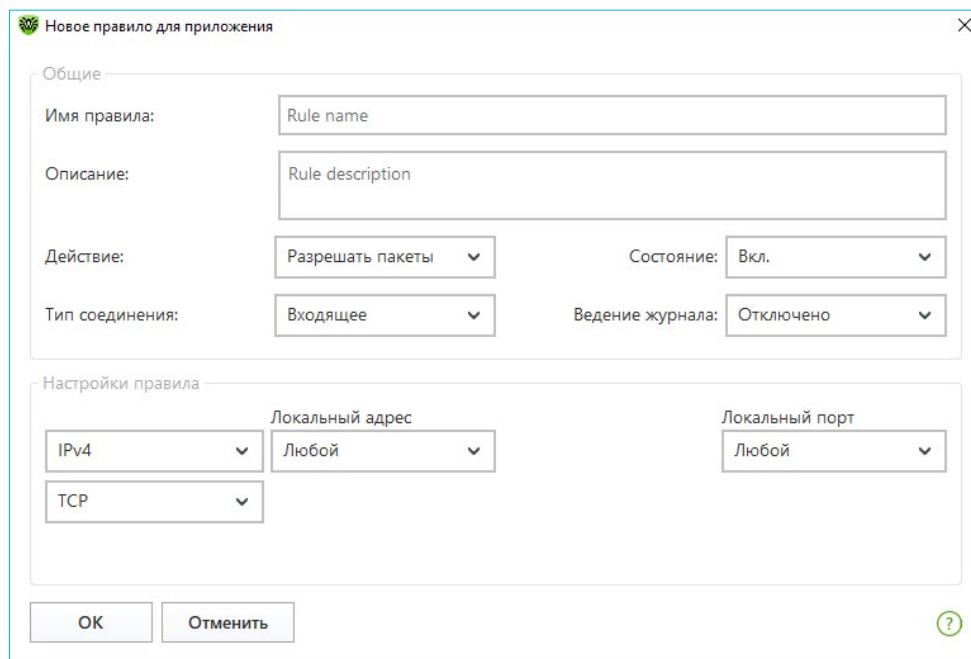
Чтобы разрешить или запретить приложению запускать другие приложения, в выпадающем списке **Запуск сетевых приложений** выберите **Разрешать** или **Запрещать**. При выборе **Не задано** на это приложение будут распространяться настройки выбранного режима работы Брандмауэра.

Выберите режим доступа к сетевым ресурсам **Разрешать все** (все соединения приложения будут разрешены), **Блокировать все** (все соединения приложения запрещены), **Не задано** (на это приложение будут распространяться настройки выбранного режима работы Брандмауэра) или **Пользовательский** — в этом режиме вы можете создать набор правил, разрешающих или запрещающих те или иные соединения приложения

Если вы выбрали **Пользовательский режим**, то вид окна создания правила изменяется, и вы можете определить правила фильтрации, регулирующие сетевое взаимодействие программы с конкретными хостами сети.



Чтобы создать правило, нажмите на кнопку  (Создать).

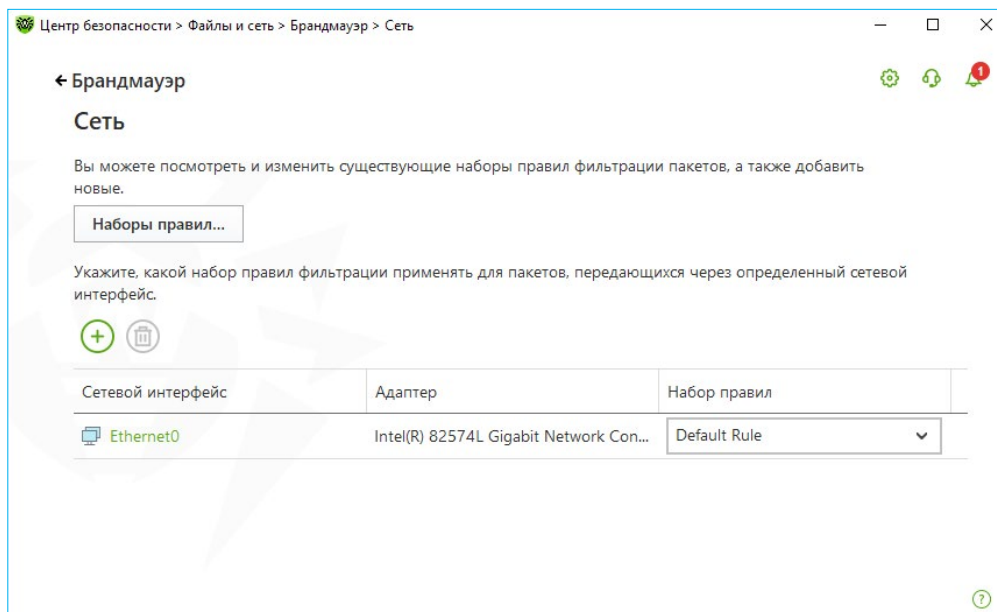


По окончании редактирования набора правил нажмите кнопку **ОК** для сохранения внесенных изменений или кнопку **Отменить** для отказа от изменений. Изменения, внесенные в набор правил, сохраняются при переключении на другой режим.

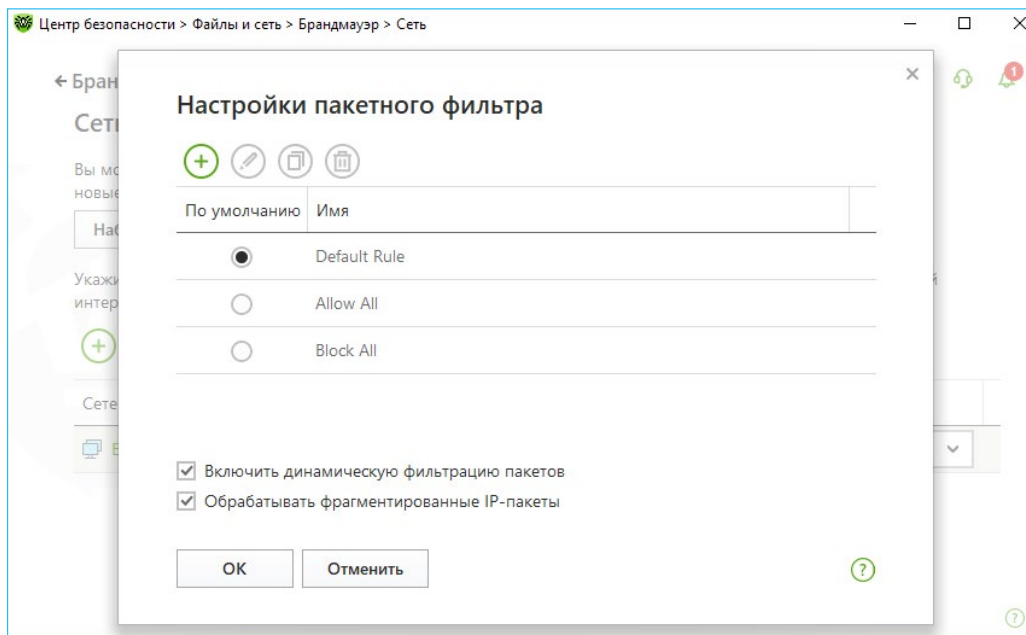
2.8.2.2. Настройка параметров работы известных сетей

В окне Брандмауэр кликните по строчке **Дополнительные настройки** и в разделе настроек **Параметры работы для известных сетей** нажмите **Изменить**.

Откроется окно со списком сетевых интерфейсов, для которых заданы правила.




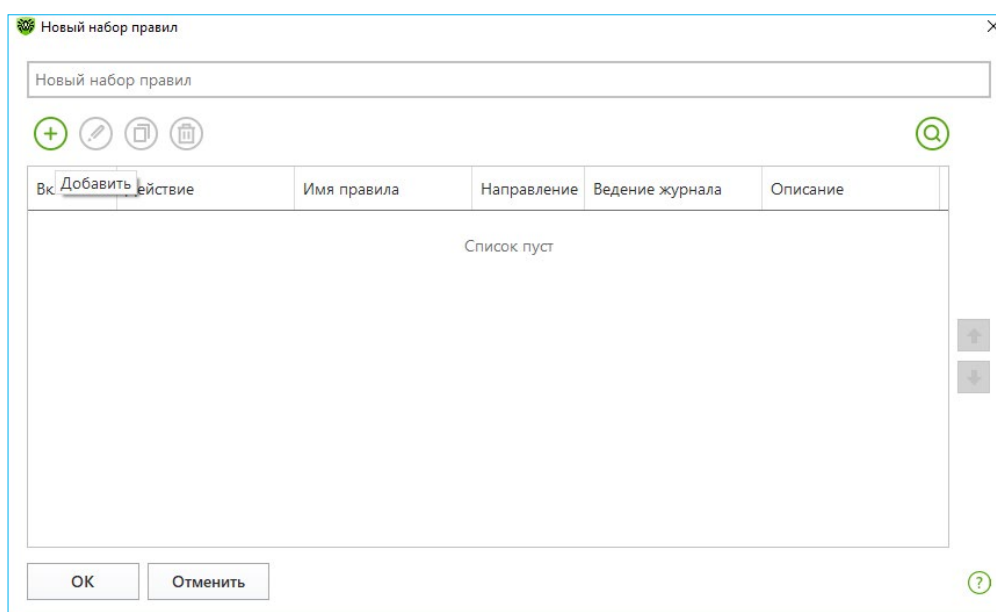
Для управления существующими наборами правил и добавления новых перейдите в окно **Настройки пакетного фильтра**, нажав кнопку **Наборы правил**.



Брандмауэр поставляется со следующими предустановленными наборами правил:


- **Default Rule** — правила, описывающие наиболее часто встречающиеся конфигурации сети и распространенные атаки (используется по умолчанию для всех новых интерфейсов);
- **Allow All** — все пакеты пропускаются;
- **Block All** — все пакеты блокируются.

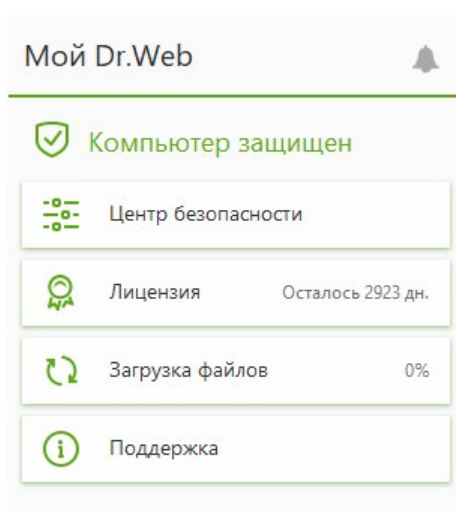
Для удобства использования и быстрого переключения между режимами фильтрации вы можете задать дополнительные наборы правил, нажав на кнопку  (Создать) или скопировав существующий набор и изменив его в режиме редактирования.




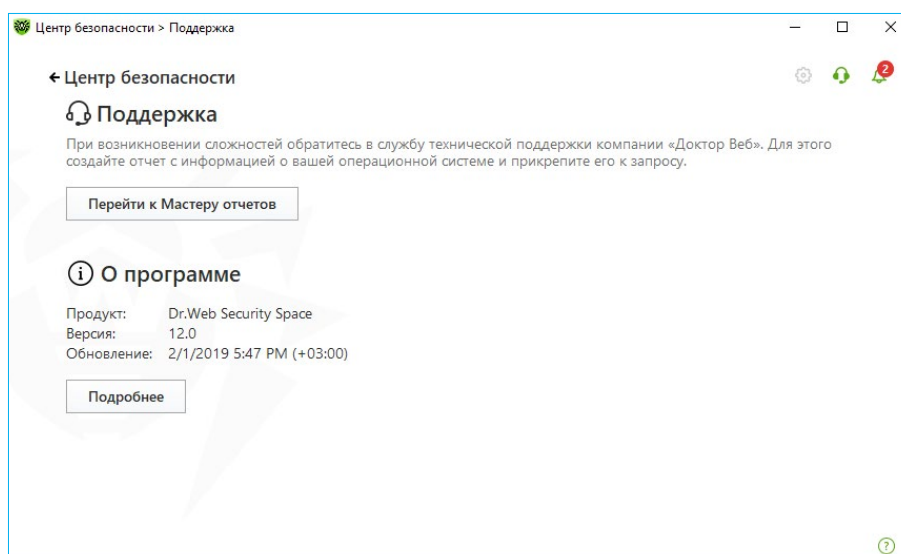
3. Типичные ошибки в настройке системы защиты

3.1. Версия антивируса

Используемая вами версия антивируса должна быть актуальной, а лицензия — действующей. Чтобы проверить актуальность лицензии, щелкните по значку  в системном трее. Напротив пункта **Лицензия** будет показано количество дней, оставшихся до истечения действующей лицензии.



Чтобы узнать используемую версию продукта, щелкните по значку , выберите пункт **Поддержка**.



Внимание! Текущая версия антивируса Dr.Web Security Space — 12. Использование неактуальных версий увеличивает риск заражения в связи с отсутствием в них новейших технологий детектирования.

Из истории продуктов Dr.Web

В версии Dr.Web Enterprise Security Suite 10 благодаря оптимизации сканирующего сервиса Dr.Web Scanning Engine была ускорена проверка объектов на наличие угроз.

Компания «Доктор Веб» в 2016 году переработала базу Офисного контроля. Количество записей в ней удалось уменьшить более чем в два раза! Размер базы нерекондуемых ресурсов снизился с 330 Мб до 165! Что, естественно, привело к ускорению работы антивируса.

Переработка вирусных баз позволила удалить 2 миллиона записей, объем вирусных баз уменьшился на треть!

Группировка записей по типам файлов позволила резко поднять скорость обработки non-PE файлов.

Старое — не значит не потребляющее ресурсов!

3.2. Отключения компонентов

*Здравствуйте, Ув. команда Dr.Web, помогите расшифровать зараженный компьютер вирусом WannaCry. Заражение произошло при открытии сайтов (какой именно сайт — не имею понятия, так как не сразу заметил, что произошло заражение), антивирус стоял... , на момент заражения был выключен, к сожалению**


Обращение в техническую поддержку

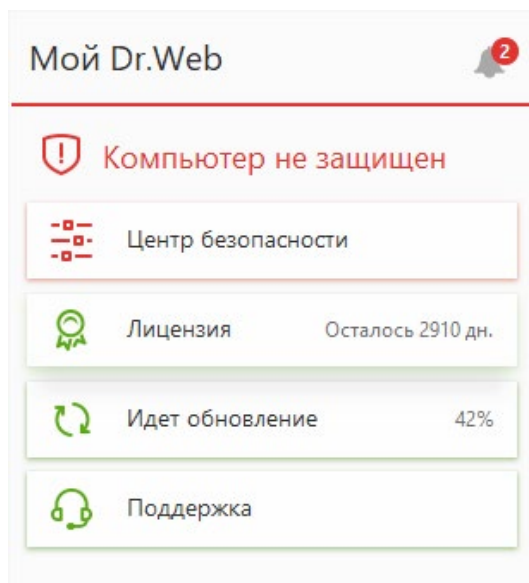
* Пользователь не использовал продукты Dr.Web.

Все компоненты антивирусной защиты на момент заражения должны быть включены. В том числе модули Превентивной защиты, Dr.Web SpIDer Gate, Антиспам и Брандмауэр.

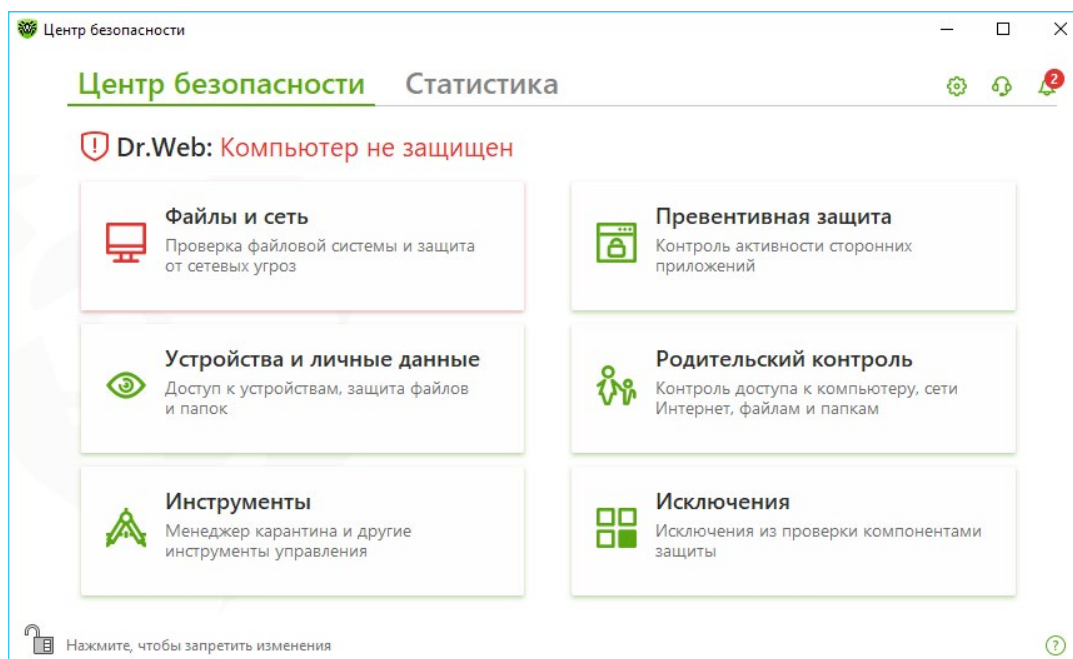
- Использование компонента Антиспам позволяет блокировать получение неизвестных вредоносных файлов по признакам распространения мошеннических писем.
- Превентивная защита (Dr.Web Process Heuristic) определяет до 99% шифровальщиков, еще не известных антивирусному ядру.
- Проверка трафика (Dr.Web SpIDer Gate) защищает от коммуникаций с сайтами, используемыми злоумышленниками.

Компонент Dr.Web SpIDer Gate доступен в составе Dr.Web Security Space, тарифном пакете Dr.Web Премиум услуги «Антивирус Dr.Web» и в лицензии Dr.Web Desktop Security Suite Комплексная защита.

Об отключении одного или нескольких компонентов свидетельствует вид значка агента в системном трее: , а само меню агента будет выглядеть так:



Внимание! Отсутствие значка агента в системном трее может означать, что антивирус выключен и защита компьютера не производится. Узнать, какие компоненты отключены, можно, кликнув по значку агента и далее выбрав пункт Центр безопасности.



Внимание! Использование компонента Антиспам позволяет блокировать получение неизвестных вредоносных файлов по признакам распространения мошеннических писем.


3.3. Отказ от обновлений

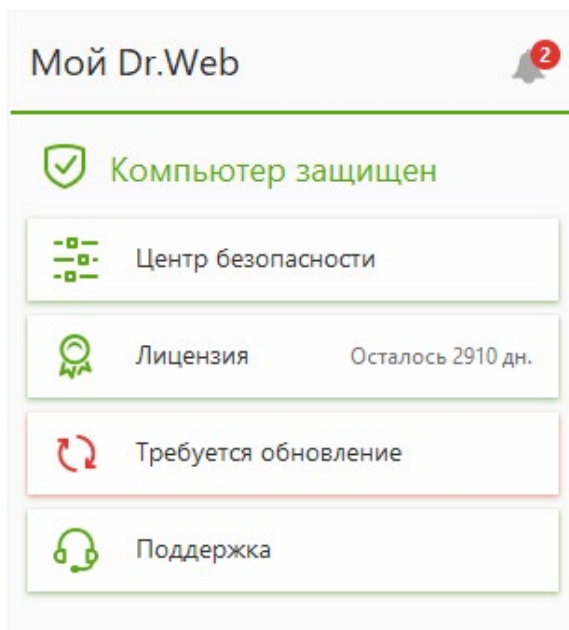
- *Добрый вечер, прошу помочь с расшифровкой моих файлов. Заражение, по-видимому, произошло из-за того, что вирусная база долго не обновлялась**
- *Заражение произошло внезапно. В результате работы за компьютером (в т. ч. в интернете) операционная система предупредила о перезагрузке в результате возникновения системной ошибки. После перезагрузки файлы постепенно зашифровывались (антивирус, который использовался, не был обновлен).**

Обращение в техническую поддержку


* Пользователь не использовал продукты Dr.Web.


Все обновления антивируса должны быть установлены, включая требующие перезагрузки в целях установки новых драйверов перехвата и исправления потенциальных уязвимостей защиты.

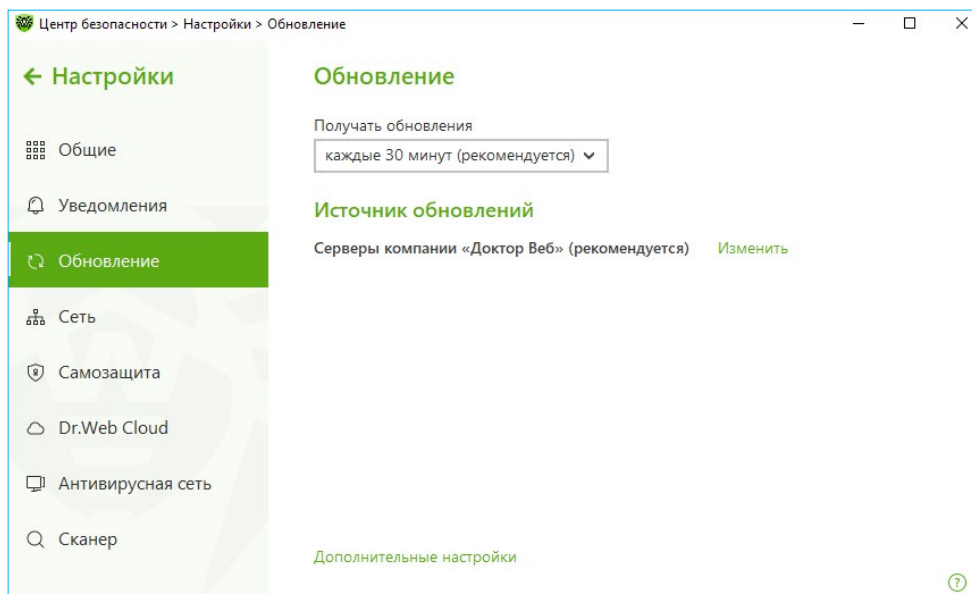
Чтобы проверить статус обновлений, кликните по значку . Статус будет показан в открывшемся меню.



Внимание! В день на анализ в антивирусную лабораторию поступает до миллиона новых вредоносных файлов. Задержка обновлений даже на несколько часов — это возможный пропуск сотен ранее не известных (в том числе для эвристики) вредоносных файлов.

Чтобы проверить периодичность получения обновлений, кликните по значку  в системном меню, затем в открывшемся меню последовательно нажмите на

Центр безопасности и значок . В открывшемся окне **Настройки** выберите **Обновление**.



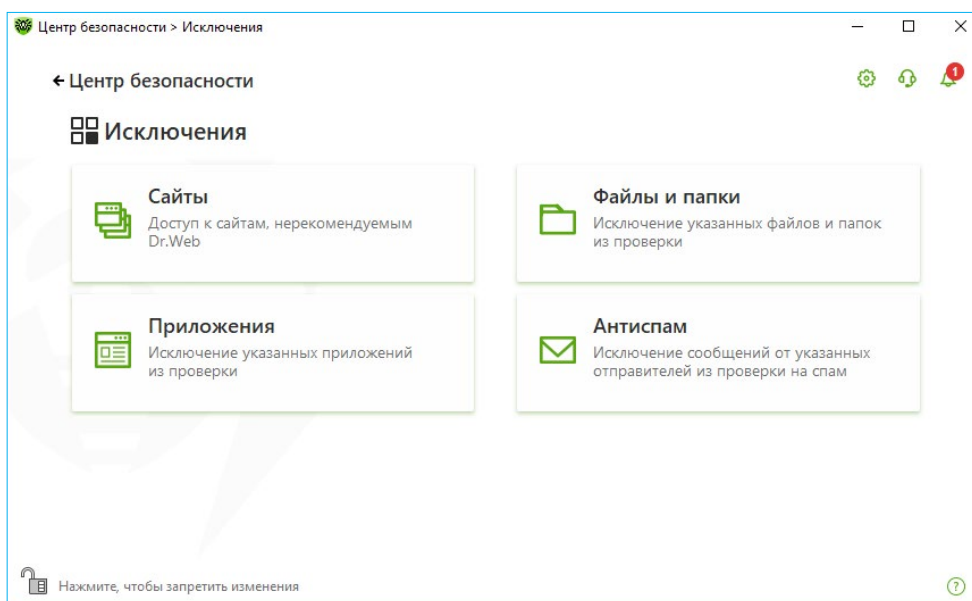
Период между обновлениями должен быть не более 1 часа.

Для перевода средств злоумышленникам требуется от одной до трех минут. Не стоит задерживать обновления антивируса.

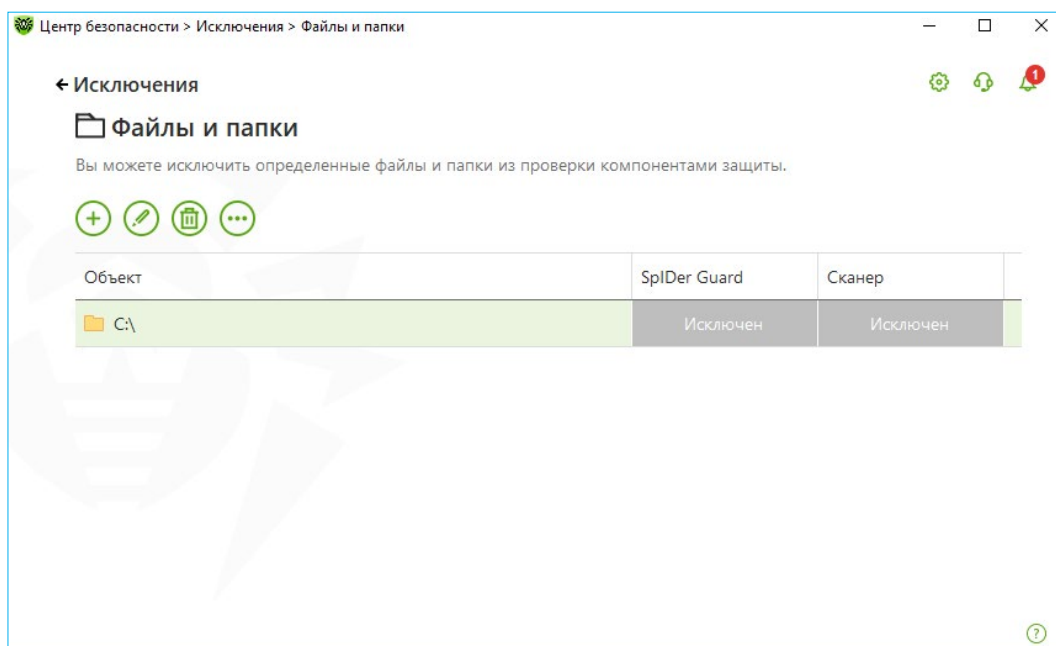
3.4. Исключения из проверки

Внимание! Компания «Доктор Веб» не рекомендует широко использовать исключения из антивирусной проверки — это помогает злоумышленникам обходить защиту вашего компьютера.

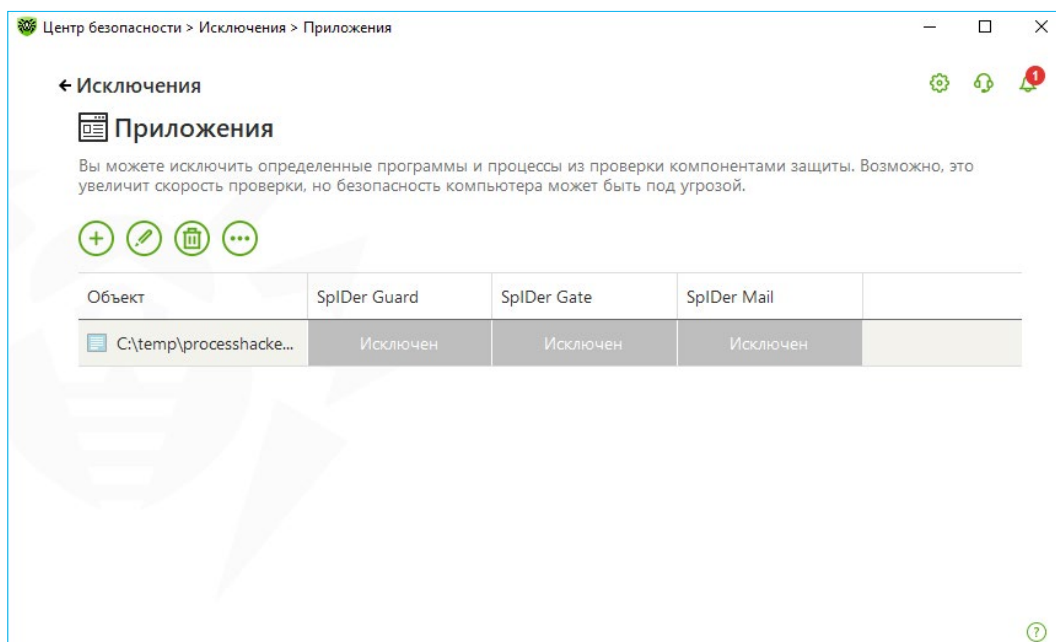
Проверить наличие исключений можно в окне Центр безопасности, выбрав раздел Исключения.



Слишком большие исключения позволят злоумышленнику бесконтрольно орудовать на компьютере — даже если антивирус знает угрозу.



Внимание! Не рекомендуется исключать проверку трафика для используемых программ — иначе никакое вредоносное ПО, загруженное данными программами, проверяться не будет.



4. Рекомендации компании «Доктор Веб» по защите компьютера от программ-шифровальщиков

Статистика показывает, что в более чем в 90% случаев жертвы запускают шифровальщиков собственными руками.

- Необходимо использовать поддерживаемую производителем операционную систему и ПО. Выпуск обновлений безопасности для неподдерживаемых систем не гарантирован!
- Необходимо работать под ограниченными правами. Минимальные права пользователей и отключение неиспользуемых сервисов существенно снижают возможности для атакующих.

Настройте права доступа к данным и сетевым папкам для всех пользователей, работающих на компьютере. В противном случае заражение компьютера может привести к шифрованию всех документов для всех пользователей — в том числе во всех сетевых папках.

WannaCry пытается удалить резервные копии зашифрованных файлов. Так как эта операция требует прав администратора, операционная система показывает предупреждение от службы UAC. Если пользователь не соглашается, резервные копии файлов не удаляются.

- Не следует соглашаться на предложения запустить вложение или открыть документ (обычно это специально сформированные злоумышленниками файлы в форматах *.doc и *.pdf, также зачастую помещаемые в архивы с форматами *.zip, *.rar, *.7z и *.cab) в связи с тем, что проверка архивов часто отключается для увеличения быстродействия.
- Используйте решения, имеющие функционал резервного копирования (создания копий файлов или всей системы). Крайне не рекомендуется создавать резервные копии копированием файлов вручную, а также хранить резервные копии на самом компьютере. Не рекомендуется хранить резервные копии на ином жестком диске или в сетевой папке, доступ к которой имеется с локального компьютера. Рекомендуется использовать съемные носители и/или облачные хранилища, а также создавать или хранить резервные копии в зашифрованном виде. Таким образом, файлы будут защищены не только от программ-шифровальщиков, но и от отказов компьютерной техники.

Внимание! До создания резервной копии следует убедиться, что копируемые файлы уже не зашифрованы и не замещают незашифрованные версии файлов.

Начиная с Windows Vista в состав ОС Windows входит служба защиты системы на всех дисках, которая создает резервные копии файлов и папок во время архивации или создания точки восстановления системы. По умолчанию эта служба включена только для системного раздела.

Внимание! Использование данной службы не защищает от действий программ-шифровальщиков, так как они могут отключать данную службу и уничтожать ранее сделанные копии.

- Не открывайте почтовые вложения от неизвестных отправителей. В большинстве случаев программы-шифровальщики распространяются именно через почту. Задача злоумышленника — убедить пользователя открыть вложение из письма или перейти по ссылке.
- Если ваши данные зашифровали, не стоит без консультации со специалистами использовать программы для расшифровки, менять расширения зашифрованных файлов и т. д. В результате этих действий вы можете окончательно потерять свои данные — их не сможет найти и восстановить даже специальная утилита расшифровки.
- Включите показ расширений файлов (см. ниже п. 4.1). Отсутствие показа расширений приводит к тому, что жертвы не видят, что на самом деле находится внутри архивов.
- Используйте только лицензионные программы.
- Своевременно устанавливайте обновления безопасности операционной системы и всех установленных на вашем компьютере программ.

Более подробная информация по действиям в случае заражения шифровальщиком расположена по адресу <http://legal.drweb.ru/encoder>.

4.1. Правила действий при инциденте с шифровальщиком

- Обратитесь в службу технической поддержки компании «Доктор Веб» (эта услуга бесплатна для пользователей коммерческих лицензий Dr.Web).
- Приложите к запросу 2–3 зашифрованных файла.
- Постарайтесь максимально подробно вспомнить обстоятельства заражения: это касается и полученных вами по электронной почте подозрительных

писем, и скаченных из Интернета программ, и сайтов, которые вы посещали. Продукты Dr.Web позволяют автоматически собрать необходимую для анализа ситуации информацию. Для этого, щелкнув по значку антивируса в системном трее, выберите пункт **Инструменты** и в появившемся окне **Инструменты** выберите **Отчет для технической поддержки**.

- Если у вас сохранилось письмо с вложением, после открытия которого файлы на компьютере оказались зашифрованными, не удаляйте его: это письмо должно помочь специалистам определить версию троянца, проникшего на ваш компьютер.
- Ни в коем случае не пытайтесь каким-либо образом изменить содержимое папок с зашифрованными файлами, не удаляйте никакие файлы, не пытайтесь восстановить зашифрованные файлы самостоятельно, не пытайтесь переустановить операционную систему.
- Не пользуйтесь зараженным ПК до получения инструкций от службы технической поддержки компании «Доктор Веб».
- Если вы запустили антивирусное сканирование, не предпринимайте каких-либо действий по лечению или удалению обнаруженных вредоносных программ — они могут понадобиться специалистам в процессе поиска ключа для расшифровки файлов.

4.2. Типичные ошибки при обнаружении действий шифровальщика и обращении в службу технической поддержки

- Если ваши файлы зашифрованы — всё уже случилось. Не нужно торопиться — потратите несколько минут и опишите ситуацию. Какую операционную систему вы используете, устанавливали ли вы обновления, что вы делали в момент заражения...

*Добрый вечер вот такой вот противный гад появился у меня на рабочем столе. Уважаемый доктор Веб. отправляю вам его скриншот.**

Обращение в техническую поддержку

Данное сообщение означает, что хозяин компьютера не заметил шифрования файлов!

** Пользователь не использовал продукты Dr.Web.*

- Если ваши файлы зашифровались – обесточьте компьютер (выньте вилку из розетки!) и дождитесь ответа технической поддержки.

*Здравствуйтесь, открыли письмо, компьютер начал виснуть, перезагрузили через какое то время, долго включался. как включился все было зашифровано. Системотехники на работе пытались его чистить и колдовать самостоятельно.**

Обращение в техническую поддержку

** Пользователь не использовал продукты Dr.Web.*

Антивирусное сканирование с последующим лечением способно уничтожить как тело троянца, так и используемые им файлы и компоненты.

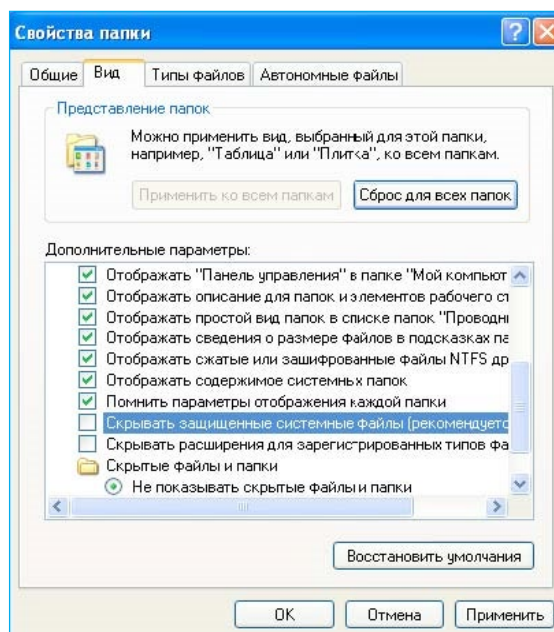
Чтобы увеличить шансы на успешное восстановление зашифрованных данных, ни в коем случае нельзя:

- менять расширение у зашифрованных файлов;
- переустанавливать систему;
- использовать самостоятельно — не имея рекомендаций специалистов технической поддержки компании «Доктор Веб» — какие-либо программы для расшифровки/восстановления данных;
- удалять/переименовывать какие-либо файлы и программы (в том числе временные);
- если было запущено антивирусное сканирование — нельзя предпринимать никаких необратимых действий по лечению/удалению вредоносных объектов.

4.3. Включение показа расширений имен файлов

Чтобы включить отображение расширений файлов:

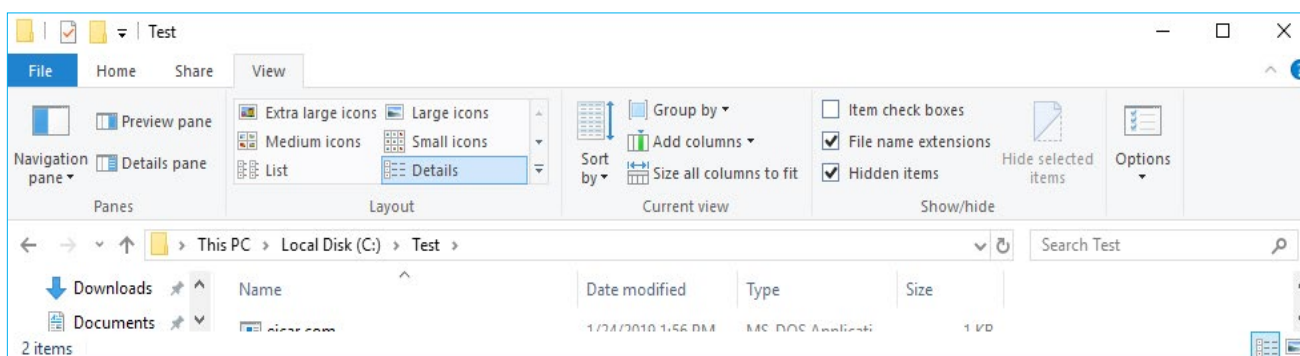
- Для **Windows XP**: в меню **Пуск** выберите **Настройки** → **Панель управления** → **Свойства папок** и снимите галочку для параметра **Скрывать расширения для зарегистрированных типов файлов**.



- Для **Windows 7**: на клавиатуре нажмите левый Alt. В появившемся меню нажмите **Сервис** → **Параметры папок**, в открывшемся окне перейдите

на вкладку **Вид** и в списке дополнительных параметров снимите галочку для параметра **Скрывать расширения для зарегистрированных типов файлов**.

- Для **Windows 8/8.1**: откройте любую папку или запустите Проводник Windows 8, нажав клавиши Windows + E. В главном меню проводника перейдите на вкладку **Вид** и установите галочку напротив строки **Расширения имен файлов** — если она отмечена, то расширения показываются (не только в выбранной папке, но и везде на компьютере), если нет — расширения скрыты.



4.4. Утилиты дешифровки

Расшифровать файлы, зашифрованные злоумышленниками, можно с помощью специальных утилит, предоставляемых службой технической поддержки компании «Доктор Веб» по запросу. К сожалению, количество появляющихся ежедневно видов троянцев-шифровальщиков не позволяет создать утилиты для каждого из них. Поэтому, если ваши файлы были зашифрованы еще не известным троянцем, можно [заказать услугу дешифровки](#). Услуга является бесплатной для владельцев действующих коммерческих лицензий Dr.Web Security Space, Dr.Web Enterprise Security Suite (Комплексная защита) и подписчиков услуги «Антивирус Dr.Web» (тарифный пакет Dr.Web Премиум) — при соблюдении ими этих [условий](#) на момент инцидента.

Если вам потребовалась услуга дешифровки, [пришлите](#) для анализа не менее 3–5 зашифрованных файлов различного типа. Кроме того, помочь дешифровке может дополнительная информация — описание процесса заражения, письмо с требованием выкупа и т. д. Если известен файл, в результате запуска которого злоумышленники смогли зашифровать ваши файлы, желательно также приложить его к запросу.

Внимание! Перед запуском утилит создайте копии зашифрованных файлов.

4.5. Где могут находиться файлы программ-шифровальщиков

Если вы обнаружили подозрительный файл, запуск которого мог привести к заражению компьютера и шифрованию файлов, — отправьте подозрительный файл на анализ. Файлы могут находиться по следующим путям:

APPDATA	ОС Windows NT/2000/XP: Диск:\Documents and Settings\%UserName%\Application Data\%USERPROFILE%\Local Settings\Application Data ОС Windows Vista/7/8: Диск:\Users\%UserName%\AppData\Roaming\%USERPROFILE%\AppData\Local
TEMP (временный каталог)	%TEMP%*.tmp %TEMP%*.tmp\ %TEMP%* %WINDIR%\Temp
Временный каталог Internet Explorer	ОС Windows NT/2000/XP: %USERPROFILE%\Local Settings\Temporary Internet Files\ ОС Windows Vista/7/8: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\ ..\temporary internet files\content.ie5\ ..\temporary internet files\content.ie5*\
Рабочий стол	%UserProfile%\Desktop\
Корзина	Диск:\Recycler\ Диск:\\$Recycle.Bin\ Диск:\\$Recycle.Bin\s-1-5-21-????????- ?????????-????????-1000 (? -- 0-9)
Системный каталог	%WinDir% %SystemRoot%\system32
Каталог документов пользователя	%USERPROFILE%\Мои документы\ %USERPROFILE%\Мои документы\Downloads
Каталог для скачивания файлов в веб-браузере	%USERPROFILE%\Downloads
Каталог автозагрузки	%USERPROFILE%\Главное меню\Программы\Автозагрузка

Внимание! Файлы Trojan.Encoder могут находиться не только в указанных выше местах.

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



© ООО «Доктор Веб»,
2003-2019



Присоединяйтесь к нам в социальных сетях

