



Руководство пользователя



© «Доктор Веб», 2025. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

Ограничение ответственности

Ни при каких обстоятельствах ООО «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

Dr.Web Katana

Версия 2.0

Руководство пользователя

15.04.2025

ООО «Доктор Веб», Центральный офис в России

Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 2, корп. 12А

Сайт: <https://www.drweb.com/>

Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах вы можете найти на официальном сайте компании.

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!



Содержание

1. Введение	6
1.1. Используемые обозначения и сокращения	6
2. О продукте	8
2.1. Компоненты защиты и модули управления	8
2.2. Методы обнаружения угроз	8
2.3. Системные требования	10
3. Установка, изменение и удаление программы	13
3.1. Установка программы	13
3.2. Изменение компонентов программы	18
3.3. Удаление и переустановка программы	21
4. Проверка работы программы	22
5. Лицензирование	23
5.1. Активация лицензии	26
5.1.1. Активация при помощи серийного номера	27
5.1.2. Активация при помощи ключевого файла	29
5.2. Продление лицензии	32
5.3. Ключевой файл	33
6. Меню программы	35
7. Центр безопасности	37
8. Обновление программных модулей	39
9. Лента уведомлений	44
10. Настройки программы	46
10.1. Общие настройки	46
10.1.1. Защита настроек программы паролем	47
10.1.2. Выбор цвета темы интерфейса	48
10.1.3. Выбор языка программы	50
10.1.4. Управление настройками Dr.Web	51
10.1.5. Ведение журнала работы Dr.Web	51
10.1.6. Настройки карантина	54
10.1.7. Автоматическое удаление записей статистики	55
10.2. Настройки уведомлений	56
10.3. Настройки обновления	60



10.4. Сеть	64
10.5. Самозащита	66
10.6. Dr.Web Cloud	67
10.7. Удаленный доступ к Dr.Web	69
11. Превентивная защита	71
11.1. Защита от вымогателей	72
11.2. Поведенческий анализ	76
11.3. Защита от эксплойтов	84
12. Защита от потери данных	87
13. Инструменты	92
13.1. Менеджер карантина	93
13.2. Антивирусная сеть	94
13.3. Менеджер лицензий	96
14. Статистика работы компонентов	99
15. Техническая поддержка	104
15.1. Помощь в решении проблем	104
15.2. О программе	107
16. Приложение А. Дополнительные параметры командной строки	108
16.1. Параметры для Модуля обновления	108
16.2. Коды возврата для Модуля обновления	111
17. Приложение Б. Угрозы и способы их обезвреживания	112
17.1. Виды компьютерных угроз	112
17.2. Действия для обезвреживания угроз	117
18. Приложение В. Принципы именования угроз	118
19. Приложение Г. Основные термины и понятия	123



1. Введение

Настоящее руководство содержит подробное описание установки продукта Dr.Web Katana, а также рекомендации по его использованию и решению типичных проблем, связанных с компьютерными угрозами. В основном рассматриваются стандартные режимы работы компонентов программы Dr.Web Katana (с настройками по умолчанию).

В Приложениях содержится общая справочная информация, а также дополнительные параметры для настройки программы Dr.Web Katana, предназначенные для опытных пользователей.

1.1. Используемые обозначения и сокращения

Условные обозначения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
<i>Антивирусная сеть</i>	Новый термин или акцент на термине в описаниях.
<IP-address>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
C:\Windows\	Наименования файлов и каталогов, фрагменты программного кода.
<u>Приложение А</u>	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

Сокращения

В тексте руководства будут употребляться без расшифровки следующие сокращения:

- Dr.Web — Dr.Web Katana;
- FTP — (от англ. File Transfer Protocol) протокол передачи файлов;
- HTTP — (от англ. Hypertext Transfer Protocol) протокол передачи гипертекста;
- POP3 — (от англ. Post Office Protocol Version 3) протокол почтового отделения, версия 3;



- SSL — (от англ. Secure Sockets Layer) уровень защищенных сокетов;
- TCP — (от англ. Transmission Control Protocol) протокол управления передачей;
- TLS — (от англ. Transport Layer Security) протокол защиты транспортного уровня;
- ОС — операционная система;
- ПО — программное обеспечение.



2. О продукте

Dr.Web Katana защищает систему от компьютерных угроз с помощью несигнатурных методов: анализирует поведение процессов, использует облачные технологии обнаружения угроз и предустановленные правила. Программа не конфликтует с антивирусами других разработчиков и может работать в паре с ними, чтобы усилить защиту компьютера.

Dr.Web Katana осуществляет контроль целостности состава продукта каждый раз при загрузке обновлений, а также непрерывно защищает собственные файлы и процессы от случайных повреждений и несанкционированного вмешательства в процессе работы. Таким образом Dr.Web Katana обеспечивает защиту от вредоносных действий, направленных на работу антивирусных программ.

Информацию о версии продукта, составе компонентов, дате последнего обновления вы можете найти на странице **Поддержка** в разделе [О программе](#).

2.1. Компоненты защиты и модули управления

Dr.Web Katana включает в состав следующие компоненты защиты и модули управления:

Компонент/модуль	Описание
Поведенческий анализ	Компонент, контролирующий доступ приложений к критически важным объектам системы и обеспечивающий целостность запущенных приложений.
Защита от эксплойтов	Компонент, блокирующий вредоносные объекты, которые используют уязвимости в приложениях.
Защита от вымогателей	Компонент, обеспечивающий защиту от программ-шифровальщиков.
Модуль обновления	Позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов Dr.Web, а также производит их автоматическую установку.
SplDer Agent	Модуль, с помощью которого осуществляется настройка и управление работой компонентов продукта.

2.2. Методы обнаружения угроз

Все антивирусные продукты, разработанные компанией «Доктор Веб», применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.



Поведенческий анализ

Методы поведенческого анализа позволяют анализировать последовательность действий всех процессов в системе. При обнаружении признаков поведения вредоносной программы действия приложения блокируются.

Dr.Web Process Heuristic

Технология поведенческого анализа Dr.Web Process Heuristic защищает от новейших, наиболее опасных вредоносных программ, которые способны избежать обнаружения традиционными сигнатурными и эвристическими механизмами.

Dr.Web Process Heuristic анализирует поведение каждой запущенной программы, сверяясь с постоянно обновляемым облачным сервисом Dr.Web, и на основе актуальных знаний о том, как ведут себя вредоносные программы, делает вывод о ее опасности, после чего принимаются необходимые меры по нейтрализации угрозы. К названиям угроз, обнаруженных при помощи Dr.Web Process Heuristic, добавляется префикс DPH.

Данная технология защиты данных позволяет свести к минимуму потери от действий неизвестной угрозы при минимальном потреблении ресурсов защищаемой системы.

Dr.Web Process Heuristic контролирует любые попытки изменения системы:

- распознает процессы вредоносных программ, изменяющих нежелательным образом пользовательские файлы (например, попытки шифрования со стороны троянских программ-шифровальщиков), в том числе расположенные в каталогах, доступных по сети;
- препятствует попыткам вредоносных программ внедриться в процессы других приложений;
- защищает от модификаций вредоносными программами критических участков системы;
- выявляет и прекращает вредоносные, подозрительные или ненадежные сценарии и процессы;
- блокирует возможность изменения вредоносными программами загрузочных областей диска с целью невозможности запуска (например, буткитов) на компьютере;
- предотвращает отключение безопасного режима Windows, блокируя изменения реестра;
- не позволяет вредоносным программам изменить правила запуска программ;
- пресекает загрузки новых или неизвестных драйверов без ведома пользователя;
- блокирует автозапуск вредоносных программ, а также определенных приложений, например анти-антивирусов, не давая им зарегистрироваться в реестре для последующего запуска;



- блокирует ветки реестра, которые отвечают за драйверы виртуальных устройств, что делает невозможной установку троянских программ под видом нового виртуального устройства;
- не позволяет вредоносному программному обеспечению нарушить нормальную работу системных служб.

Dr.Web ShellGuard

Технология Dr.Web ShellGuard защищает компьютер от *эксплойтов* — вредоносных объектов, пытающихся использовать уязвимости с целью получения контроля над атакуемыми приложениями или операционной системой в целом. К названиям угроз, обнаруженных при помощи Dr.Web ShellGuard, добавляется префикс

DPH:Trojan.Exploit.

Dr.Web ShellGuard защищает распространенные приложения, устанавливаемые на компьютеры под управлением Windows:

- интернет-браузеры (Internet Explorer, Mozilla Firefox, Google Chrome и др.);
- приложения MS Office;
- системные приложения;
- приложения, использующие java-, flash- и pdf-технологии;
- медиапроигрыватели.

Анализируя потенциально опасные действия, система защиты благодаря технологии Dr.Web ShellGuard опирается не только на прописанные правила, хранящиеся на компьютере, но и на знания облачного сервиса Dr.Web, в котором собираются:

- данные об алгоритмах программ с вредоносными намерениями;
- информация о заведомо чистых файлах;
- информация о скомпрометированных цифровых подписях известных разработчиков программного обеспечения;
- информация о цифровых подписях рекламных или потенциально опасных программ;
- информация о нежелательных для посещения сайтах;
- алгоритмы защиты тех или иных приложений.

2.3. Системные требования

Использование программы Dr.Web возможно на компьютере, удовлетворяющем следующим требованиям:

Параметр	Требования
Процессор	С поддержкой системы команд i686



Параметр	Требования
Операционная система	Для 32-разрядных операционных систем: • Windows XP с пакетом обновлений SP2 или более поздними; • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10 21H2 или более ранняя; • Windows Server 2003 с пакетом обновлений SP1 или более поздними; • Windows Server 2008. Для 64-разрядных операционных систем: • Windows Vista с пакетом обновлений SP2 или более поздними; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10 21H2 или более ранняя; • Windows 11; • Windows Server 2008 с пакетом обновлений SP2 или более поздними; • Windows Server 2008 R2; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019; • Windows Server 2022
Оперативная память	Не менее 100 МБ
Разрешение экрана	Не менее 1024 × 768



Поскольку компания Microsoft прекратила поддержку алгоритма хеширования SHA-1, перед установкой программы Dr.Web Katana на Windows Vista, Windows 7, Windows Server 2008 или Windows Server 2008 R2 необходимо убедиться, что система поддерживает алгоритм хеширования SHA-256. Для этого установите все рекомендуемые обновления из Центра обновления Windows. Подробную информацию о необходимых пакетах обновлений вы можете найти на [официальном сайте компании «Доктор Веб»](#)

Стабильная и безошибочная работа Dr.Web не гарантируется на оборудовании с нестандартной конфигурацией, такой как разогнанные процессоры, измененные параметры памяти и напряжения питания.



Для обеспечения правильной работы Dr.Web должны быть открыты следующие порты:

Назначение	Направление	Номера портов
Для активации и продления лицензии	исходящий	443
Для обновления (если включена опция обновления по https)	исходящий	443
Для обновления	исходящий	80
Для соединения с облачным сервисом Dr.Web Cloud	исходящие	2075 (в том числе для UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)



3. Установка, изменение и удаление программы

Перед началом установки Dr.Web Katana ознакомьтесь с [системными требованиями](#). Также рекомендуется выполнить следующие действия:

- установить все критические обновления, выпущенные компанией Microsoft для вашей версии операционной системы (подробнее об обновлении); если поддержка операционной системы производителем прекращена, рекомендуется перейти на более современную версию операционной системы;
- проверить при помощи системных средств файловую систему и устранить обнаруженные проблемы;
- закрыть активные приложения.

Установка Dr.Web возможна в одном из следующих режимов:

- в режиме командной строки;
- в режиме мастера установки.

3.1. Установка программы



Установка Dr.Web должна выполняться пользователем с правами администратора данного компьютера.

Установка в режиме мастера установки

Чтобы запустить установку в обычном режиме, воспользуйтесь одним из следующих методов:

- если у вас имеется установочный файл (`drweb-2.0-katana-win.exe`), запустите его;
- если у вас имеется фирменный диск с установочным комплектом, вставьте диск в привод. Если для привода включен режим автозапуска диска, процедура установки запустится автоматически. Если режим автозапуска отключен, запустите на выполнение файл `autorun.exe`, расположенный на диске. Откроется окно, содержащее меню автозапуска. Нажмите кнопку **Установить**.

Следуйте указаниям программы установки. На любом шаге до начала копирования файлов на компьютер вы можете выполнить следующее:

- чтобы вернуться к предыдущему шагу программы установки, нажмите кнопку **Назад**;
- чтобы перейти на следующий шаг программы, нажмите кнопку **Далее**;
- чтобы прервать установку, нажмите кнопку **Отменить**.



Чтобы установить программу



Перед началом установки проверяется актуальность установочного файла. В случае если существует более новый установочный файл, вам будет предложено его скачать.

1. На первом шаге установки вы можете подключиться к [облачным сервисам Dr.Web](#), которые позволяют осуществлять проверку данных, используя наиболее свежую информацию об угрозах, которая обновляется на серверах компании «Доктор Веб» в режиме реального времени. Опция включена по умолчанию.



Рисунок 1. Мастер установки

2. Если вы хотите произвести установку с параметрами по умолчанию, перейдите к следующему пункту. Чтобы выбрать устанавливаемые компоненты, указать путь установки и некоторые дополнительные параметры, нажмите ссылку **Параметры установки**.

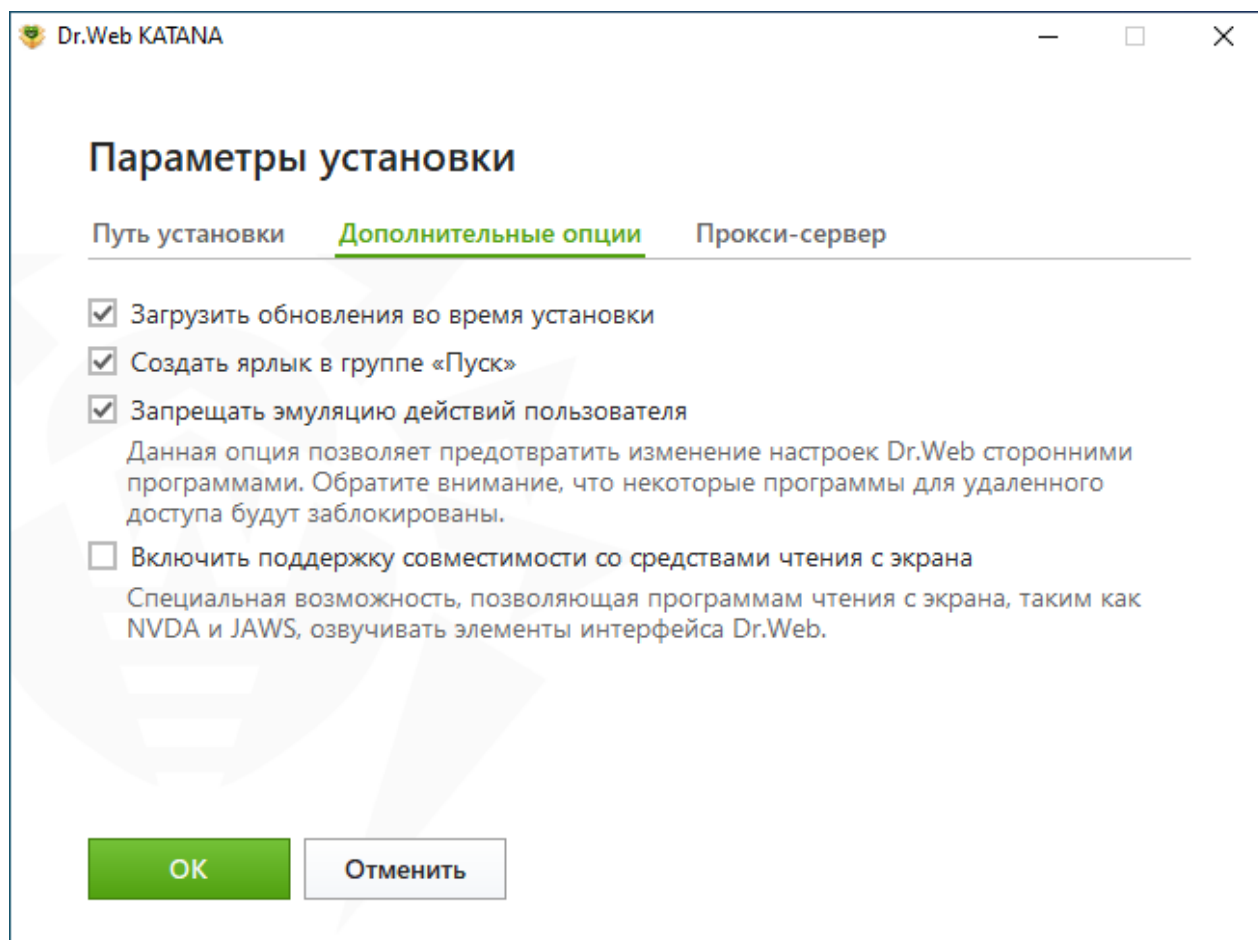


Рисунок 2. Параметры установки

Данная опция предназначена для опытных пользователей.

- На первой вкладке вы можете изменить путь установки. По умолчанию это папка DrWeb, расположенная в папке Program Files на системном диске. Для изменения пути установки нажмите кнопку **Обзор** и укажите необходимый путь.
- На второй вкладке окна вы можете установить флажок **Загрузить обновления во время установки**, чтобы в процессе установки были загружены актуальные модули антивируса. Вы можете установить флажок **Включить поддержку совместимости со средствами чтения с экрана**, чтобы использовать программы экранного доступа, такие как JAWS и NVDA, для озвучивания элементов интерфейса Dr.Web. Эта функция делает интерфейс программы доступным для людей с ограниченными возможностями. Также вам будет предложено настроить создание ярлыков для запуска программы Dr.Web.
- При необходимости укажите параметры прокси-сервера.

Чтобы сохранить изменения, нажмите кнопку **ОК**. Чтобы выйти из окна, не сохраняя изменений, нажмите кнопку **Отменить**.

3. Нажмите кнопку **Далее**. Обратите внимание, что тем самым вы принимаете условия лицензионного соглашения.
4. В окне **Мастер регистрации** необходимо выбрать одну из следующих опций:



- если у вас есть [ключевой файл](#) и он находится на жестком диске или съемном носителе, выберите **Указать путь к действующему ключевому файлу**. Нажмите кнопку **Обзор** и выберите нужный ключевой файл в открывшемся окне. Подробнее вы можете прочитать в инструкции [Активация при помощи ключевого файла](#);
- для продолжения установки без ключевого файла выберите **Получить лицензию позднее**. В этом случае ни один компонент программы не будет работать до тех пор, пока вы не укажете действительный ключевой файл. Вы сможете приобрести лицензию и получить действующий ключевой файл после установки продукта.

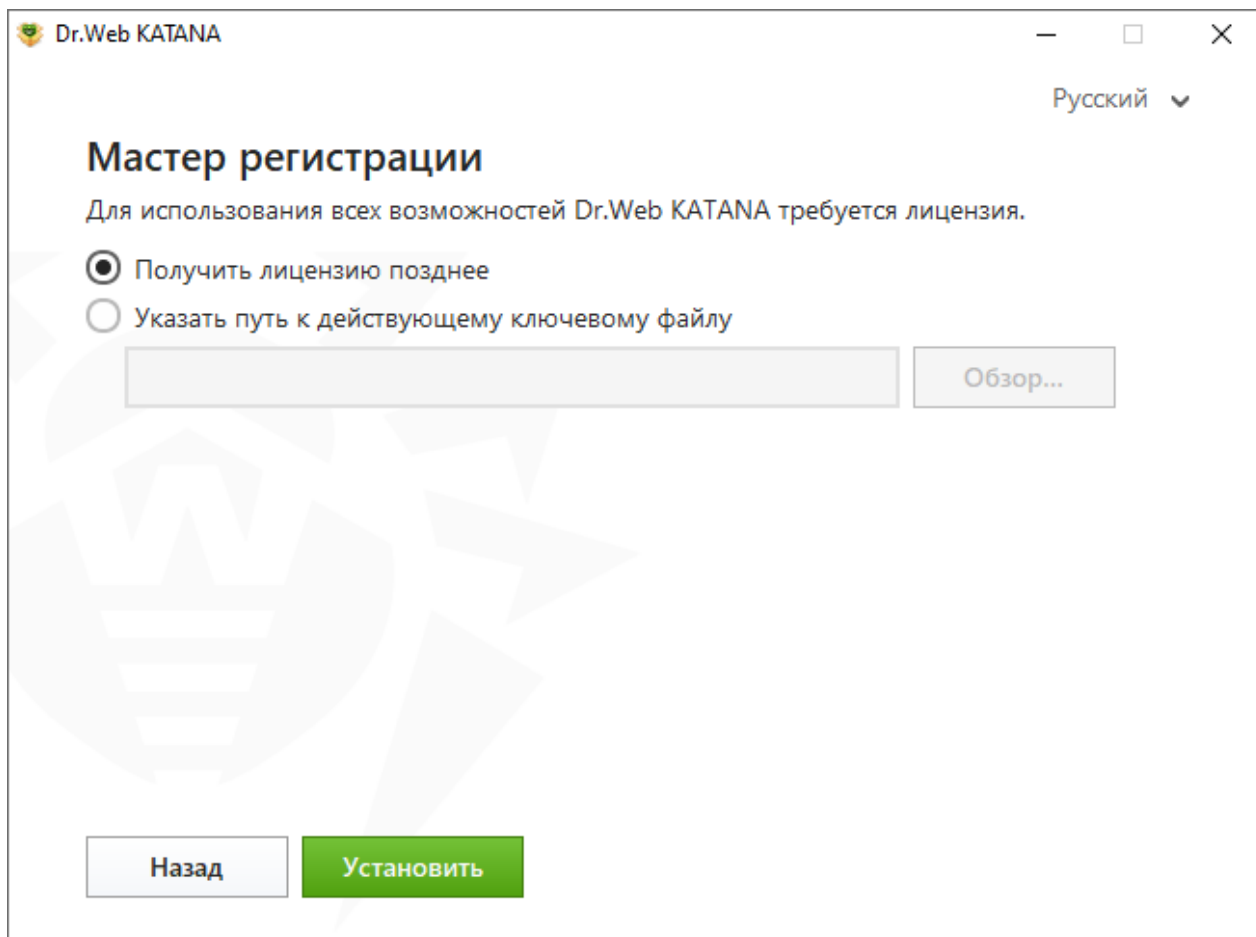


Рисунок 3. Мастер регистрации

Нажмите кнопку **Установить**.

5. Если в процессе установки вы указали действующий ключевой файл и не снимали флажок **Загрузить обновления во время установки**, будет выполнен процесс обновления компонентов программы Dr.Web. Обновление проводится автоматически и не требует дополнительных действий.
6. Чтобы завершить установку, перезагрузите компьютер.



Установка в режиме командной строки

Для запуска установки Dr.Web в фоновом режиме введите в командной строке имя исполняемого файла с необходимыми параметрами:

Параметр	Значение
lang	Язык продукта. Значение параметра — код языка в формате ISO 639-1, например, /lang ru.
reboot	Автоматическая перезагрузка компьютера после завершения установки. Может принимать значение yes или no.
silent	Установка в фоновом режиме. Может принимать значение yes или no.
blockEmulateUserActions	Включение опции Запрещать эмуляцию действий пользователя во время установки. Может принимать значение yes или no.
allowUiAccessibility	Включение опции совместимости со средствами чтения с экрана. Может принимать значение yes или no.
importSettings	Импорт настроек из файла (максимальный размер файла — 20 МБ). Необходимо указать путь к файлу.
enableDebugLogs	Ведение журнала отладки. Может принимать значение yes или no. Журнал ведется для Модуля обновлений и службы Dr.Web. Ведение журнала отключается при перезагрузке компьютера после завершения установки.

Например, при запуске следующей команды будет проведена установка Dr.Web в фоновом режиме и проведена перезагрузка после установки:

```
drweb-2.0-win-katana.exe /silent yes /reboot yes
```

Ошибка службы BFE при установке программы Dr.Web

Для функционирования некоторых компонентов программы Dr.Web необходимо наличие запущенной службы базового модуля фильтрации (BFE). В случае если данная служба отсутствует или повреждена, установка Dr.Web будет невозможна. Повреждение или отсутствие службы BFE может указывать на наличие угроз безопасности вашего компьютера.



Если попытка установки программы Dr.Web завершилась с ошибкой службы BFE, выполните следующие действия:

1. Просканируйте систему при помощи лечащей утилиты CureIt! от компании «Доктор Веб». Скачать утилиту вы можете на сайте:
<https://free.drweb.com/download+cureit+free/>.
2. Восстановите службу BFE. Для этого вы можете воспользоваться [утилитой](#)  для устранения проблем в работе брандмауэра от компании Microsoft (для операционных систем Windows 7 и выше).
3. Запустите Мастер установки Dr.Web и произведите установку согласно штатной процедуре, приведенной выше.

Если проблема не устранена, обратитесь в службу технической поддержки компании «Доктор Веб».

3.2. Изменение компонентов программы

Изменение компонентов программы осуществляется через Мастер удаления/изменения компонентов. Вы можете открыть Мастер удаления/изменения компонентов двумя способами:

- при наличии установочного файла запустите его;
- из Панели управления Windows:
 1. Выберите (в зависимости от операционной системы):

Операционная система	Последовательность действий			
Windows XP	Меню «Пуск»	Пуск → Панель управления → Установка и удаление программ		
	Классическое меню «Пуск»	Пуск → Настройка → Панель управления → Установка и удаление программ		
Windows Vista	Меню «Пуск»	Пуск → Панель управления	Классический вид	Программы и компоненты



Операционная система	Последовательность действий			
			Домашняя страница	Программы → Программы и компоненты
	Классическое меню «Пуск»	Пуск → Настройка → Панель управления → Программы и компоненты		
Windows 7	Пуск → Панель управления	Мелкие/крупные значки: Программы и компоненты		
		Категория: Программы → Удаление программ		
Windows 8, Windows 8.1, Windows 10, Windows 11	Панель управления	Мелкие/крупные значки: Программы и компоненты		
		Категория: Программы → Удаление программ		

- В списке установленных программ выберите строку **Dr.Web KATANA**.
- Нажмите кнопку **Изменить**.

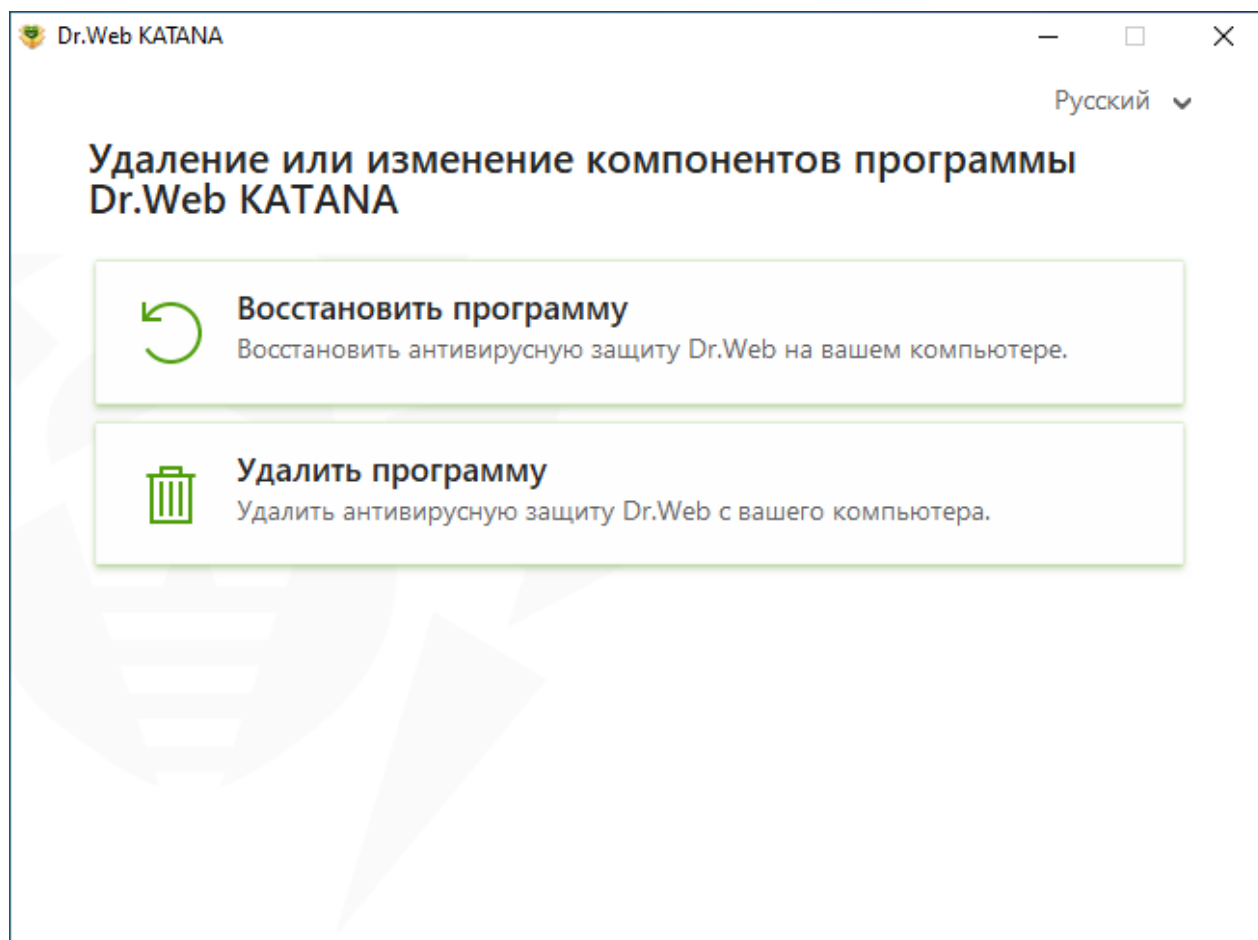


Рисунок 4. Мастер удаления/изменения компонентов

В окне Мастера удаления/изменения компонентов программы доступны следующие опции:

- **Восстановить программу**, если необходимо восстановить антивирусную защиту на вашем компьютере. Эта функция применяется в том случае, когда некоторые из компонентов программы Dr.Web были повреждены.
- **Удалить программу**, чтобы удалить все установленные компоненты.



3.3. Удаление и переустановка программы

Удаление Dr.Web



После удаления Dr.Web ваш компьютер не будет защищен от угроз.

При наличии установочного файла вы можете пропустить шаги 1–3. Запустите установочный файл и перейдите к [шагу 4](#).

1. В открывшемся списке выберите строку с названием программы.
2. Нажмите кнопку **Удалить**.
3. В окне **Сохраняемые параметры** установите флажки напротив того, что следует сохранить после удаления программы. Сохраненные объекты и настройки могут использоваться программой при повторной установке. По умолчанию выбраны все опции — **Карантин** и **Настройки Dr.Web KATANA**. Нажмите кнопку **Далее**.
4. Откроется окно **Отключение Самозащиты**, в котором необходимо ввести изображенный код подтверждения, после чего нажать кнопку **Удалить программу**.
5. Изменения вступят в силу после перезагрузки компьютера. Процесс перезагрузки можно отложить, нажав кнопку **Перезагрузить позже**. Нажмите кнопку **Перезагрузить сейчас** для немедленного завершения процедуры удаления или изменения состава компонентов Dr.Web.

Переустановка Dr.Web

1. Загрузите актуальный дистрибутив программы с [официального сайта компании «Доктор Веб»](#) . Для этого необходимо ввести действительный серийный номер в соответствующее поле.
2. Удалите продукт, [как описано выше](#).
3. Перезагрузите компьютер.
4. Заново [установите программу](#), используя загруженный дистрибутив (drweb-2.0-win-katana.exe). На этапе установки укажите путь к ключевому файлу.
5. Перезагрузите компьютер.



4. Проверка работы программы

Проверка целостности

После установки Dr.Web целостность программы поддерживается динамически в процессе ее работы и во время загрузки обновлений следующими способами:

- [Самозащита](#) непрерывно защищает файлы и процессы Dr.Web от несанкционированных изменений.
- [Модуль обновления](#) выполняет проверку целостности компонентов программы по контрольным суммам загружаемых файлов во время каждого обновления.

Чтобы проверить целостность Dr.Web, не дожидаясь запуска обновления, вы можете воспользоваться опцией [Восстановить программу](#) в окне Мастера удаления/изменения компонентов.



5. Лицензирование

Права пользователя на использование Dr.Web регулируются лицензией, приобретенной на сайте компании «Доктор Веб» или у партнеров. Лицензия позволяет полноценно использовать все возможности продукта на протяжении всего срока действия. Лицензия регулирует права пользователя, установленные в соответствии с [Лицензионным соглашением](#) , условия которого пользователь принимает во время установки программы.

Каждой лицензии сопоставлен уникальный *серийный номер*, а на локальном компьютере пользователя с лицензией связывается специальный файл, регулирующий работу Dr.Web в соответствии с параметрами лицензии. Этот файл называется лицензионным *ключевым файлом*. Подробнее о ключевом файле см. в разделе [Ключевой файл](#).

Если перед приобретением лицензии вы хотите ознакомиться с продуктом, вы можете воспользоваться его пробной версией в течение *демонстрационного периода*. При этом будут доступны все функции и компоненты продукта. Получить пробную версию Dr.Web для одного и того же компьютера можно не чаще одного раза в год, при этом автоматически формируется ключевой файл.



Пробная версия не может быть активирована и использована на Windows XP.

Способы активации лицензии

Активировать коммерческую лицензию вы можете одним из следующих способов:

- во время установки продукта при помощи Мастера регистрации;
- в любой момент работы продукта при помощи Менеджера лицензий;
- на официальном сайте компании «Доктор Веб» по адресу <https://products.drweb.com/register/>.

Активация лицензии в Мастере регистрации возможна только при помощи ключевого файла. Активация лицензии в Менеджере лицензий возможна при помощи серийного номера или ключевого файла.

Подробнее об активации лицензии см. в разделах [Активация при помощи серийного номера](#) и [Активация при помощи ключевого файла](#).

Демонстрационный период

Пользователям продуктов Dr.Web доступна лицензия на демонстрационный период сроком на 1 месяц. Пробную версию можно получить непосредственно в окне



Менеджера лицензий или в окне Активации лицензии, не указывая персональных данных.



Пробная версия не может быть активирована и использована на Windows XP.

Если у вас остались вопросы по лицензированию, ознакомьтесь со [списком наиболее частых вопросов](#)  на сайте компании «Доктор Веб».

Возможные вопросы

Как я могу перенести лицензию на другой компьютер?

Вы можете перенести вашу коммерческую лицензию на другой компьютер при помощи ключевого файла или серийного номера. Если вы хотите перенести лицензию на компьютер, на котором используется Windows XP, вы можете это сделать только при помощи ключевого файла.

Чтобы перенести лицензию на другой компьютер

- при помощи серийного номера:
 1. Скопируйте серийный номер с компьютера, с которого вы хотите перенести лицензию.
 2. Удалите Dr.Web с компьютера, с которого вы хотите перенести лицензию, или активируйте другую лицензию на этом компьютере.
 3. Активируйте текущую лицензию на компьютере, на который вы хотите перенести лицензию. Для этого воспользуйтесь Менеджером лицензий во время работы продукта (см. [Активация при помощи серийного номера](#)).
- при помощи ключевого файла:
 1. Скопируйте ключевой файл с компьютера, с которого вы хотите перенести лицензию. По умолчанию [ключевой файл](#) хранится в папке установки Dr.Web и имеет расширение `.key`.
 2. Удалите Dr.Web с компьютера, с которого вы хотите перенести лицензию, или активируйте другую лицензию на этом компьютере.
 3. Активируйте текущую лицензию на компьютере, на который вы хотите перенести лицензию. Для этого воспользуйтесь Мастером регистрации во время установки продукта или Менеджером лицензий в любое время работы продукта (см. [Активация при помощи ключевого файла](#)).



Нельзя перенести на другой компьютер лицензию, которую вы получили в рамках демонстрационного периода.

Я забыл регистрационный email. Как я могу его восстановить?

Если вы забыли адрес электронной почты, который вы указывали во время регистрации, вам необходимо обратиться в службу технической поддержки компании «Доктор Веб» по адресу <https://support.drweb.com>.

Если вы сделаете запрос с адреса, отличающегося от того, на который зарегистрирована ваша лицензия, специалист технической поддержки может попросить предоставить фото- или скан-копию лицензионного сертификата, чек об оплате лицензии, письмо интернет-магазина и другие подтверждающие документы.

Как я могу изменить регистрационный email?

Если вам необходимо изменить адрес электронной почты, который вы указывали при регистрации, воспользуйтесь специальным сервисом замены электронной почты по адресу https://products.drweb.com/register/change_email.

Почему в моем продукте отсутствует часть компонентов?

- При установке продукта были установлены не все входящие в лицензию компоненты.

Чтобы включить недостающие компоненты

1. Перейдите в раздел Панели управления Windows, посвященный установке и удалению программ.
2. В списке установленных программ выберите строку с названием программы.
3. Нажмите кнопку **Изменить**, при этом откроется окно Мастера удаления/изменения компонентов программы.
4. Выберите опцию **Изменить компоненты**.
5. Выберите из списка компонентов те компоненты, которые вы хотите включить, и нажмите кнопку **Применить**.

Либо запустите установочный файл `drweb-2.0-win-katana.exe` и в открывшемся окне выберите опцию **Изменить компоненты**. Перейдите к шагу 5.



5.1. Активация лицензии

Чтобы использовать все функции и компоненты программы, необходимо активировать лицензию. Активация лицензии возможна при помощи:

- [серийного номера](#),
- [ключевого файла](#).

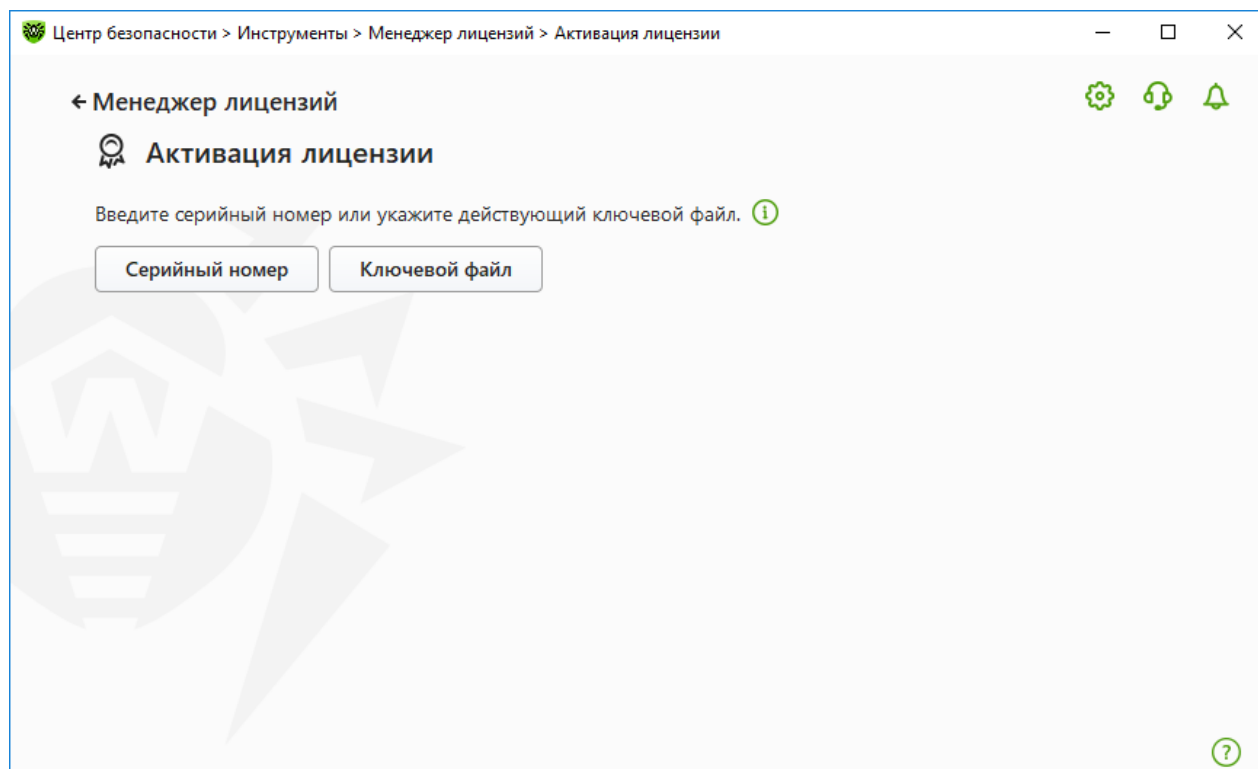


Рисунок 5. Активация лицензии

Пользователи Windows XP могут [активировать лицензию](#) только при помощи ключевого файла.



Если вы уже являлись пользователем Dr.Web, то вы сможете [продлить действие](#) приобретенной лицензии.

Активация лицензии на Windows XP

Пользователи Windows XP могут активировать лицензию только при помощи ключевого файла. Если ключевого файла нет, но есть серийный номер, его необходимо зарегистрировать на [сайте компании «Доктор Веб»](#) . После завершения процесса регистрации вам будет предоставлена ссылка для скачивания ключевого файла. Используйте этот ключевой файл для активации лицензии во время установки или в любое время работы продукта при помощи Мастера регистрации, который входит в состав Менеджера лицензий:



1. В меню Dr.Web  выберите пункт **Лицензия**. Откроется окно Менеджера лицензий. Нажмите кнопку **Активировать**.
2. В открывшемся окне нажмите кнопку **Обзор**, чтобы указать путь к ключевому файлу.
3. Нажмите кнопку **ОК**, чтобы закрыть окно и вернуться к Менеджеру лицензий.



Пробная версия не может быть активирована и использована на Windows XP.

Повторная активация

Повторная активация лицензии может потребоваться в случае утраты ключевого файла.



В случае повторной активации лицензии (в том числе пробной версии) выдается тот же ключевой файл, который был выдан ранее, при условии, что срок его действия не истек.

При переустановке продукта или если лицензия предоставляет право установки продукта на несколько компьютеров, повторная активация серийного номера не требуется.

Получить лицензионный ключевой файл через Менеджер лицензий можно ограниченное количество раз. Если это число превышено, то ключевой файл можно получить, подтвердив регистрацию своего серийного номера на сайте <https://products.drweb.com/register/>. Ключевой файл будет выслан на адрес электронной почты, который был указан при первой регистрации.

5.1.1. Активация при помощи серийного номера

Если у вас есть серийный номер, вы можете:

- активировать лицензию в любое время работы продукта при помощи Менеджера лицензий:
 1. В меню Dr.Web  выберите пункт **Лицензия**. Откроется окно Менеджера лицензий. Нажмите кнопку **Активировать**.
 2. Откроется окно Активации лицензии. Нажмите кнопку **Серийный номер**.

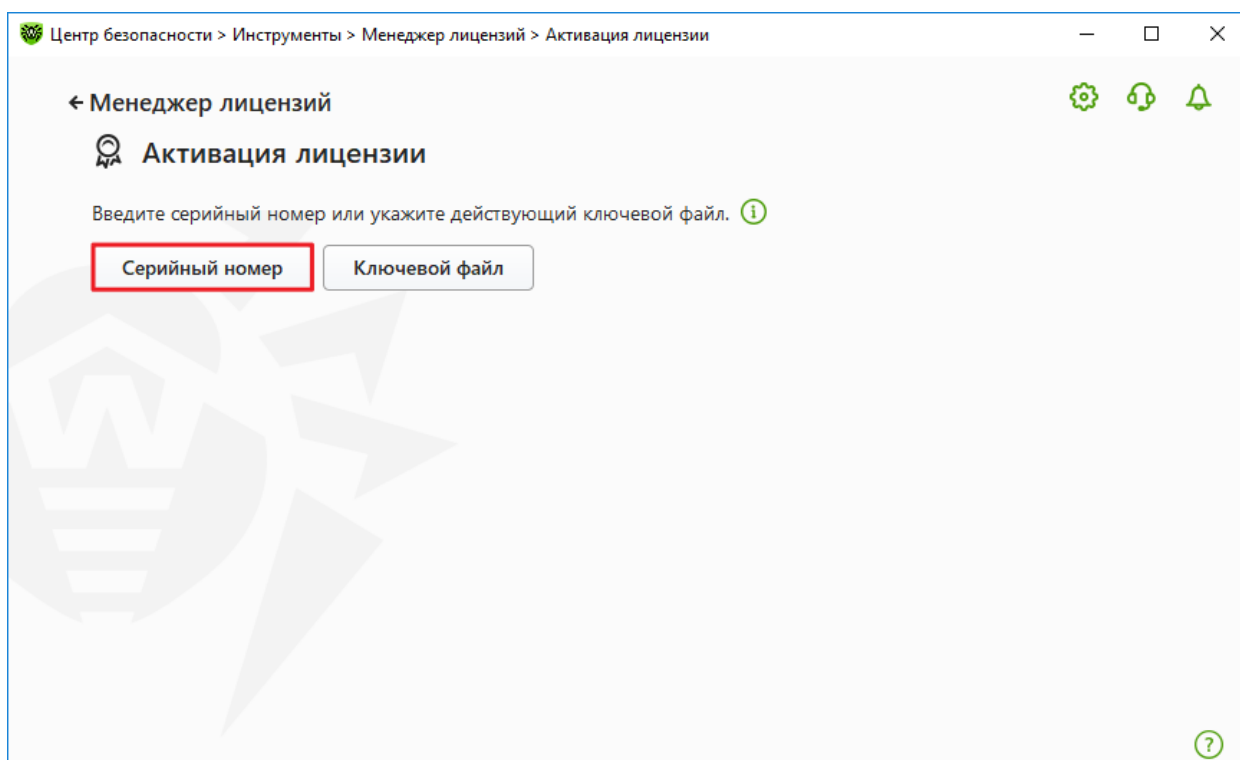


Рисунок 6. Доступ к окну ввода серийного номера

3. В новом окне введите серийный номер и нажмите **Активировать**.

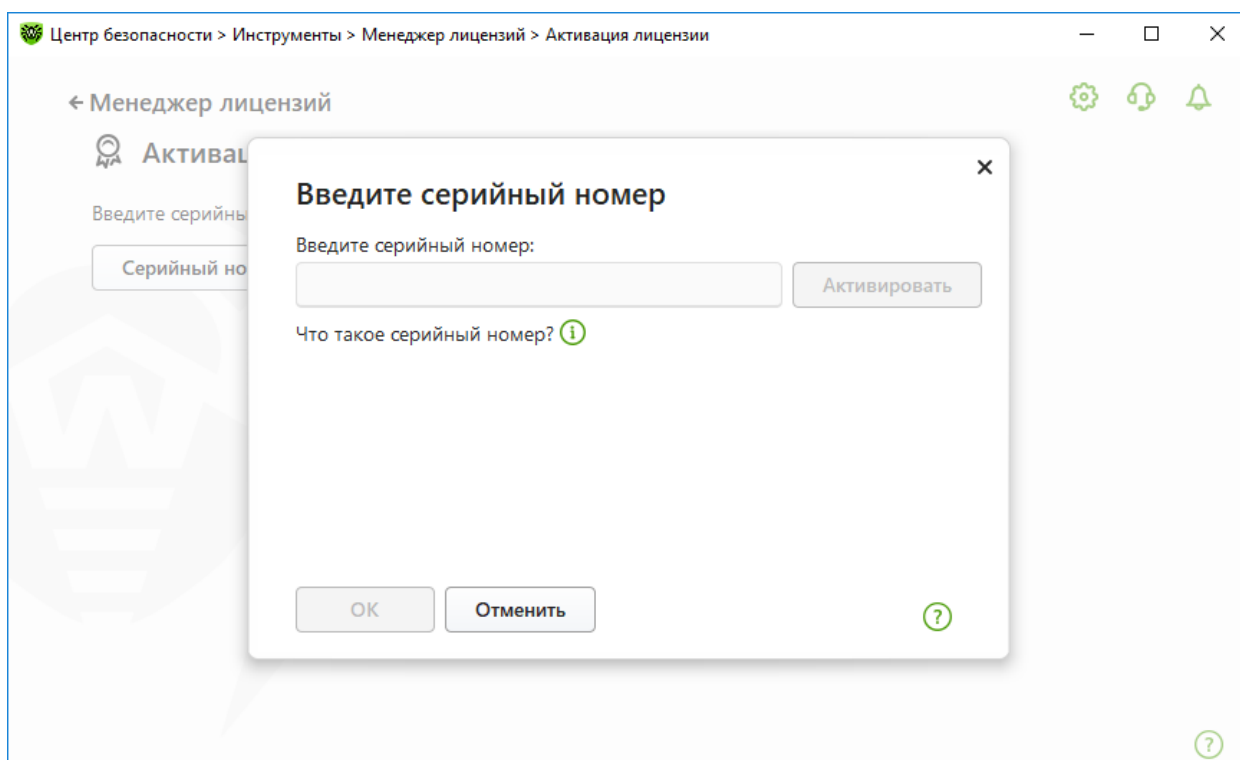


Рисунок 7. Активация при помощи серийного номера

4. Откроется страница сайта компании «Доктор Веб», на которой нужно ввести свои регистрационные данные. Следуйте инструкциям на сайте для завершения регистрации.



При длительном ожидании окно активации автоматически закроется с выводением сообщения об ошибке.

Не закрывайте окно активации до завершения регистрации серийного номера. Если по какой-либо причине окно было закрыто, лицензию можно будет активировать только с помощью [ключевого файла](#).

5. На указанный вами электронный адрес будет отправлена ссылка для регистрации серийного номера. Перейдите по ней, чтобы завершить активацию лицензии.
6. При успешной активации в окне программы появится подробная информация о лицензии. Нажмите кнопку **ОК**, чтобы закрыть окно и вернуться к Менеджеру лицензий.

Если активация лицензии завершилась неудачно, выводится сообщение об ошибке. Проверьте подключение к интернету и нажмите кнопку **Повторить**.

- зарегистрировать серийный номер на [сайте компании «Доктор Веб»](#)  и получить ключевой файл, с помощью которого вы сможете активировать лицензию.

5.1.2. Активация при помощи ключевого файла

Если у вас есть ключевой файл, вы можете активировать лицензию:

- во время установки продукта при помощи Мастера регистрации:
 1. Запустите установку продукта. На [5 шаге](#) установки выберите пункт **Указать путь к действующему ключевому файлу**. Нажмите **Установить**.

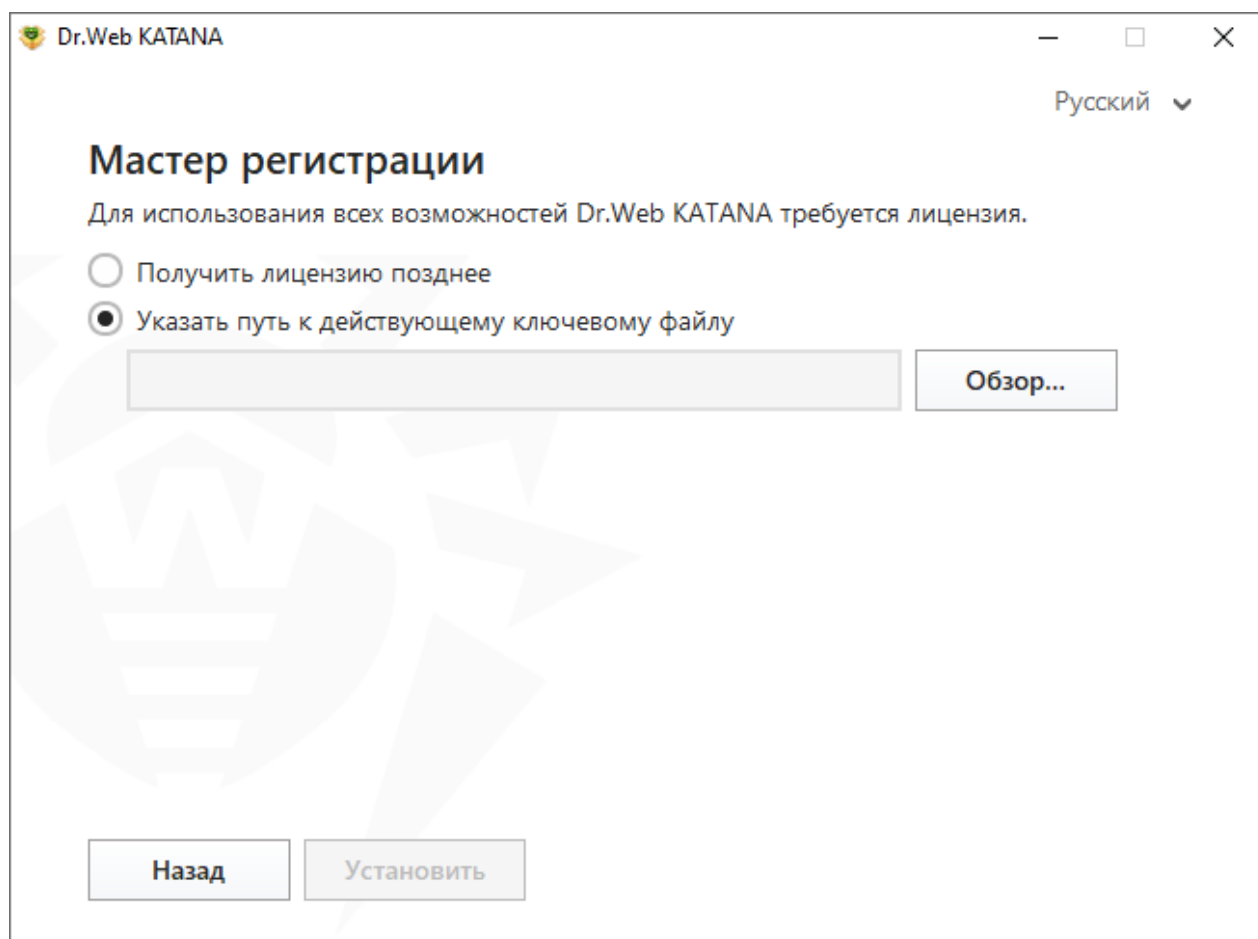


Рисунок 8. Установка. Мастер регистрации

2. Продолжите установку продукта, следуя инструкциям Мастера установки.
- в любое время работы продукта при помощи Менеджера лицензий:
 1. В меню Dr.Web  выберите пункт **Лицензия**. Откроется окно Менеджера лицензий. Нажмите кнопку **Активировать**.
 2. Откроется окно Активации лицензии. Нажмите кнопку **Ключевой файл**.

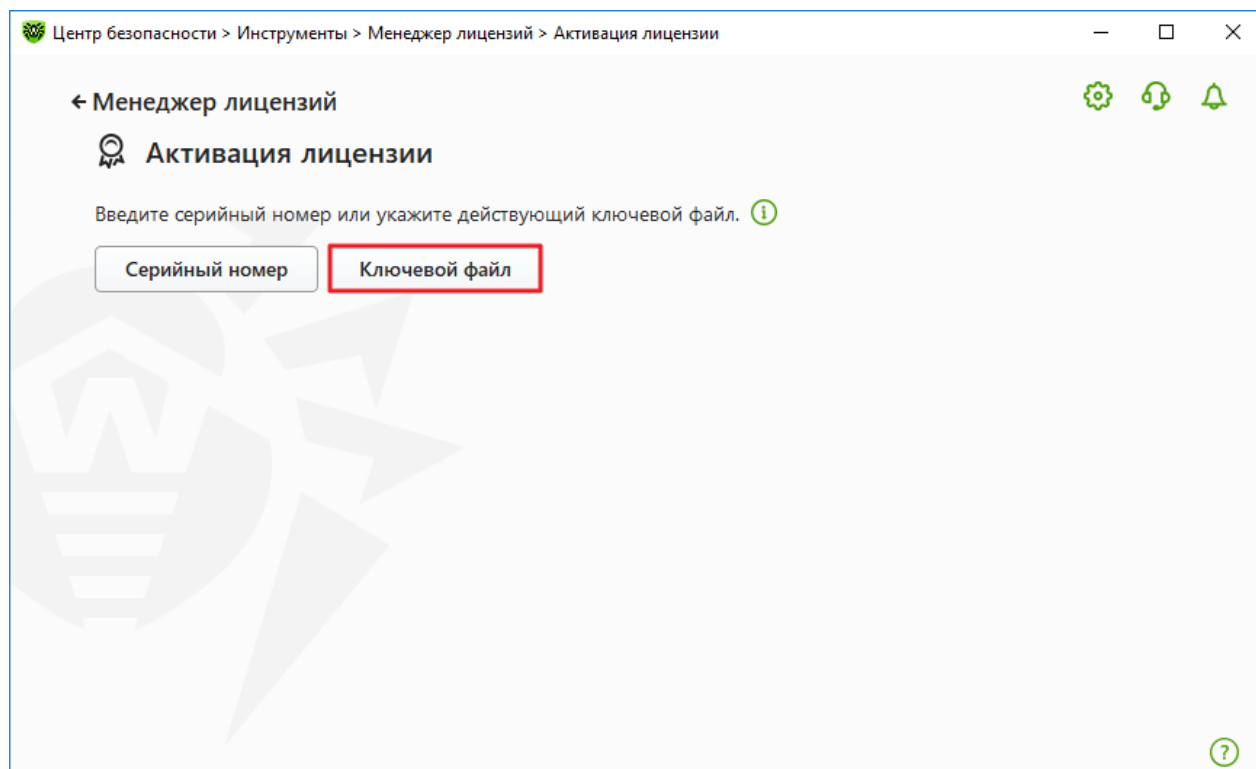


Рисунок 9. Доступ к окну ввода ключевого файла

3. В открывшемся окне нажмите кнопку **Обзор**, чтобы указать путь к ключевому файлу.

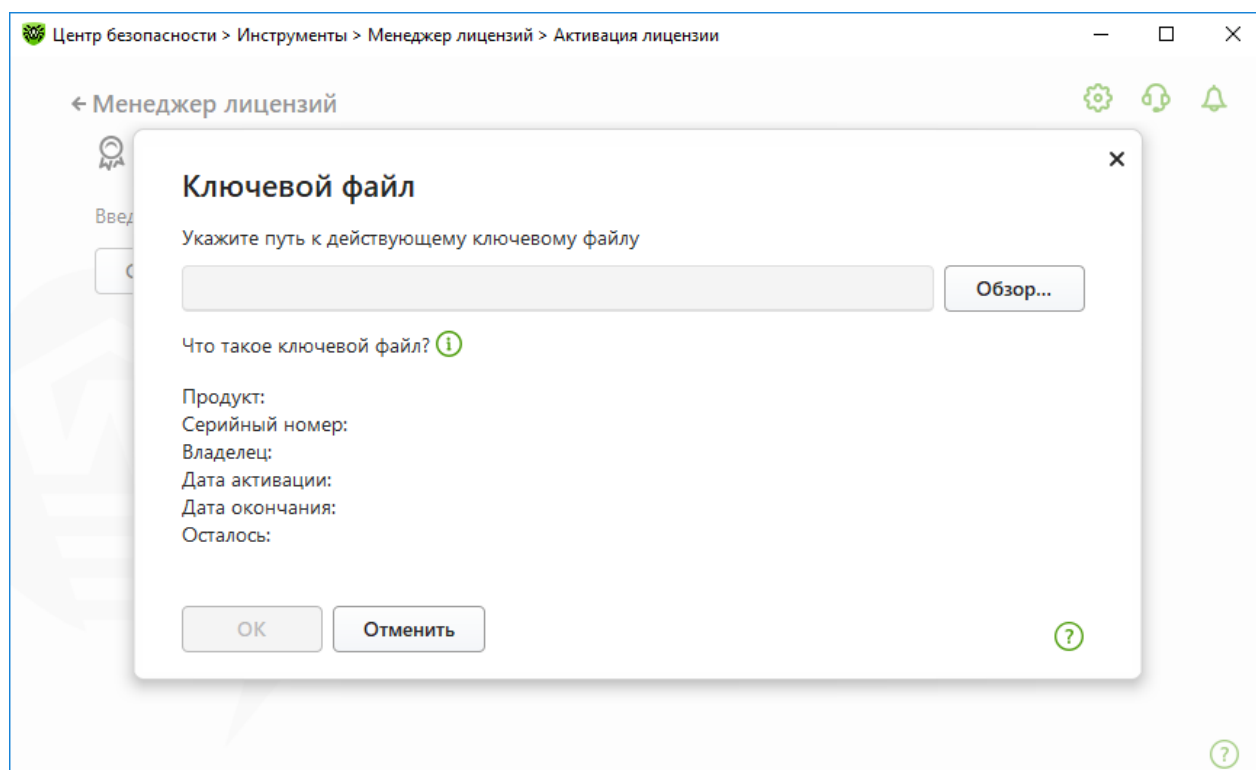


Рисунок 10. Активация при помощи ключевого файла

4. Нажмите кнопку **ОК**, чтобы закрыть окно и вернуться к Менеджеру лицензий.



5.2. Продление лицензии

Вы можете продлить текущую лицензию с помощью Мастера продлений на [сайте компании «Доктор Веб»](#)

Чтобы продлить текущую лицензию при помощи Менеджера лицензий

1. Откройте [меню](#) Dr.Web и выберите пункт **Лицензия**.
2. В окне Менеджера лицензий нажмите кнопку **Купить**. Откроется страница сайта компании «Доктор Веб», на которой вы можете оформить продление действия лицензии.

Dr.Web поддерживает обновление на лету, при котором не требуется переустанавливать Dr.Web или прерывать его работу. Чтобы обновить лицензию на использование Dr.Web, вам необходимо активировать новую лицензию.



При длительном ожидании окно активации автоматически закроется с выводением сообщения об ошибке.

Не закрывайте окно активации до завершения продления. Если по какой-либо причине окно было закрыто, лицензию можно будет активировать только с помощью [ключевого файла](#).

Если продление лицензии завершилось неудачно, выводится сообщение об ошибке. Проверьте подключение к интернету и нажмите кнопку **Повторить**.

Чтобы активировать лицензию

1. Откройте окно Менеджера лицензий, выбрав пункт **Лицензия** в [меню](#) Dr.Web . Нажмите кнопку **Активировать**.
2. В открывшемся окне нажмите кнопку **Серийный номер** или **Ключевой файл**. Введите серийный номер или укажите путь к ключевому файлу. Пользователи Windows XP могут [активировать лицензию](#) только при помощи ключевого файла.

Подробные инструкции по активации лицензии доступны в разделах [Активация при помощи серийного номера](#) и [Активация при помощи ключевого файла](#).

Если срок действия лицензии, которую вы хотите продлить, закончился, Dr.Web начнет использовать новую лицензию.

Если срок действия лицензии, которую вы хотите продлить, еще не закончился, то количество оставшихся дней будет автоматически добавлено к новой лицензии. При этом старая лицензия будет заблокирована, и вам придет соответствующее уведомление на адрес электронной почты, который вы указывали при регистрации. Рекомендуется также [удалить старую лицензию](#) при помощи Менеджера лицензий.



Если у вас остались вопросы по продлению лицензии, ознакомьтесь со [списком наиболее частых вопросов](#)  на сайте компании «Доктор Веб».

Возможные вопросы

После продления лицензии я получил письмо, что мой ключевой файл будет заблокирован через 30 дней.

Если срок действия лицензии, которую вы продлили, еще не закончился, то количество оставшихся дней автоматически добавляется к новой лицензии. При этом лицензия, на основе которой было сделано продление, блокируется. При использовании заблокированной лицензии компоненты Dr.Web не работают, и не происходит обновление.

Рекомендуется удалить старую лицензию из продукта. Для этого:

1. В [режиме администратора](#) в [меню](#) Dr.Web  выберите пункт **Лицензия**. Откроется окно Менеджера лицензий.
2. Нажмите кнопку **Подробнее**, при этом откроется окно Сведений о лицензии.
3. В выпадающем списке выберите лицензию, на основе которой было сделано продление, и нажмите кнопку .

5.3. Ключевой файл

Права пользователя на использование Dr.Web хранятся в специальном файле, называемом *ключевым файлом*. При получении ключевого файла в комплекте дистрибутива продукта установка ключевого файла производится автоматически и никаких дополнительных действий не требует.

Ключевой файл имеет расширение `.key` и содержит следующую информацию:

- перечень компонентов, которые разрешено использовать данному пользователю;
- период, в течение которого разрешено использование антивируса;
- наличие или отсутствие технической поддержки;
- другие ограничения (в частности, количество компьютеров, на которых разрешено использовать антивирус).



При работе программы ключевой файл по умолчанию должен находиться в папке установки Dr.Web. Программа регулярно проверяет наличие и корректность ключевого файла. Во избежание порчи ключа не модифицируйте ключевой файл.

При отсутствии действительного ключевого файла активность всех компонентов Dr.Web блокируется.



Ключевой файл Dr.Web является действительным при одновременном выполнении следующих условий:

- срок действия лицензии не истек;
- целостность ключа не нарушена.

При нарушении любого из условий ключевой файл становится недействительным.

Если при установке Dr.Web вы не указали путь к ключевому файлу, используется временный ключевой файл. Такой ключевой файл обеспечивает полную функциональность компонентов программы Dr.Web. Однако в [меню](#) Dr.Web  будет отсутствовать пункт **Обновление**. Обновления не будут загружаться до тех пор, пока вы не активируете лицензию или пробную версию либо с помощью Менеджера лицензий не укажете путь к действительному ключевому файлу.

Рекомендуется сохранять ключевой файл до истечения срока действия лицензии или пробной версии.



Ключевой файл, полученный для активации пробной версии, может использоваться только на том компьютере, на котором вы проходили регистрацию.



6. Меню программы

После установки программы Dr.Web в область уведомлений Windows добавляется значок , который также отражает [состояние программы](#). Чтобы открыть меню Dr.Web, нажмите значок . Если программа не запущена, в меню **Пуск** раскройте группу **Dr.Web** и выберите пункт **Центр безопасности**.

В меню Dr.Web  вы можете увидеть статус защиты, а также получить доступ к основным средствам управления и настройкам программы.



Для доступа к параметрам компонентов и для перехода к онлайн-сервису Мой Dr.Web необходимо ввести пароль, если в [настройках](#) вы включили опцию **Защищать настройки Dr.Web паролем**.

Если вы забыли пароль к настройкам продукта, обратитесь в [службу технической поддержки](#) .

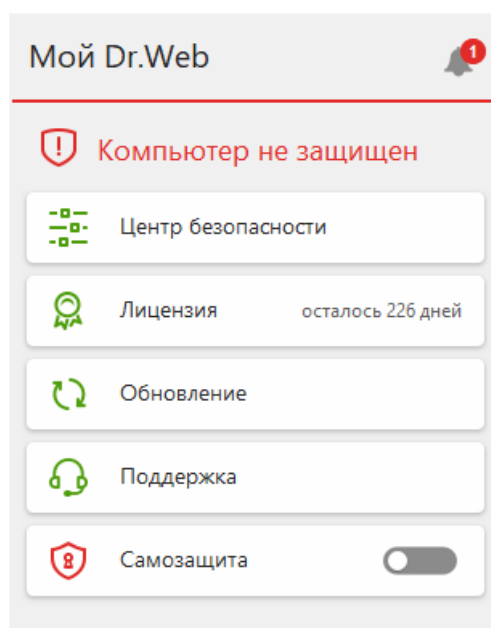


Рисунок 11. Меню программы

Пункты меню программы

Мой Dr.Web. Открывает вашу персональную страницу на сайте компании «Доктор Веб». На данной странице вы сможете получить информацию об имеющихся лицензиях (срок действия, серийный номер), продлить срок действия лицензии, задать вопрос службе технической поддержки и многое другое.

Статус защиты компьютера. При всех работающих компонентах программы отображается статус **Компьютер защищен**. При отключении одного или нескольких компонентов защиты статус меняется на **Компьютер не защищен**.



Центр безопасности. Открывает окно с доступом к основным настройкам, параметрам компонентов защиты.

Лицензия. Информация о количестве дней, оставшихся до окончания действия лицензии. Открывает [Менеджер лицензий](#).

Обновление. Информация о времени последнего обновления. Запускает обновление компонентов программы.

Поддержка. Открывает окно поддержки.

Самозащита (появляется при отключении Самозащиты). С помощью переключателя вы можете снова включить Самозащиту.

Кнопка **Лента уведомлений** . Открывает окно [Лента уведомлений](#).

Возможные состояния программы

Значок Dr.Web отражает текущее состояние программы:

Значок Dr.Web	Описание
	Все компоненты, необходимые для защиты компьютера, запущены и работают правильно.
	Самозащита или хотя бы один из компонентов отключены. Включите Самозащиту или отключенный компонент.
	Ожидается запуск компонентов после старта операционной системы, дождитесь запуска компонентов программы; либо в процессе запуска одного из ключевых компонентов Dr.Web возникла ошибка. Проверьте наличие действительного ключевого файла и при необходимости установите его.



7. Центр безопасности

Окно **Центр безопасности** предоставляет доступ ко всем компонентам, инструментам, статистике и настройкам программы.

Чтобы перейти к окну Центр безопасности

1. Откройте [меню](#) Dr.Web .
2. Выберите пункт **Центр безопасности**.

Чтобы перейти к окну Центр безопасности из меню Пуск

1. В меню **Пуск** раскройте группу **Dr.Web**.
2. Нажмите **Центр безопасности**.

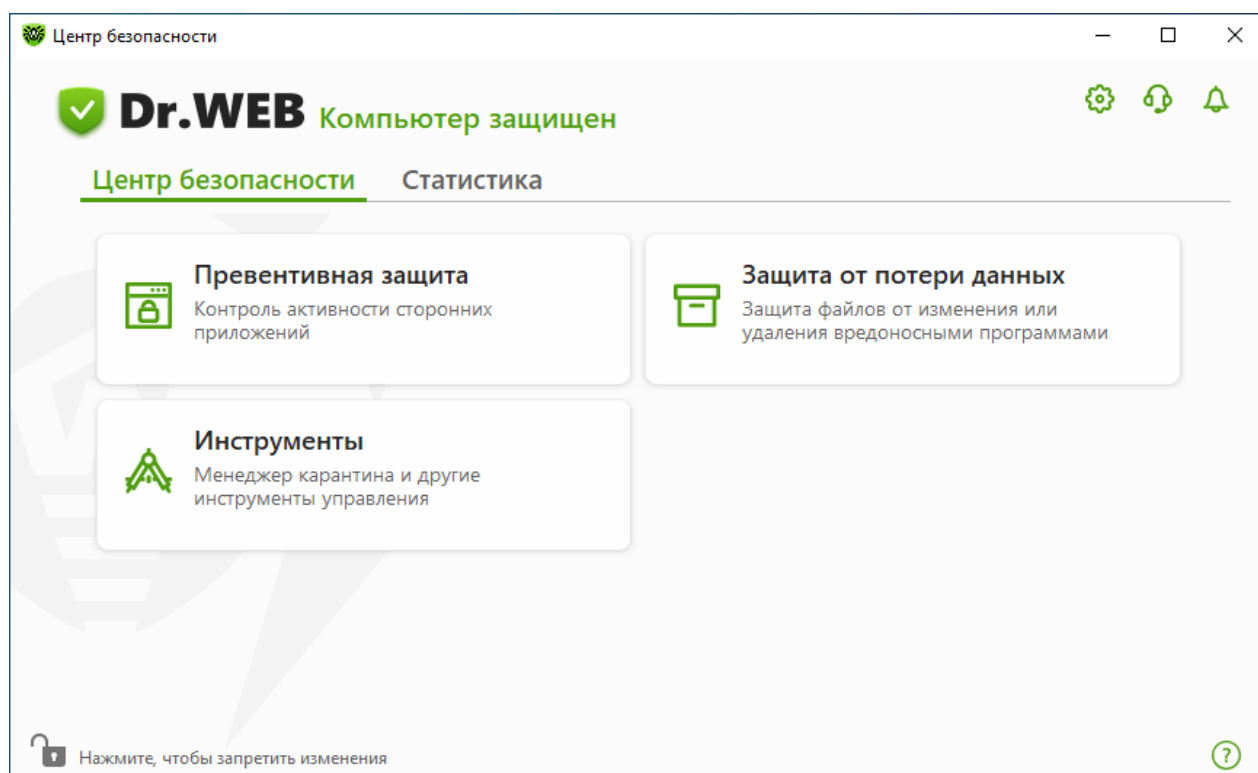


Рисунок 12. Окно Центр безопасности

Группы настроек

Из основного окна предоставляется доступ к следующим группам настроек:

- Основная вкладка **Центр безопасности** — доступ ко всем компонентам защиты и инструментам:
 - [Превентивная защита](#);
 - [Защита от потери данных](#);



▫ [Инструменты](#):

- Вкладка [Статистика](#) — статистика по основным событиям работы программы;
- Кнопка  в верхней части окна — доступ к [настройкам программы](#);
- Кнопка  в верхней части окна — доступ к окну **Поддержка**, где вы можете собрать [отчет для службы технической поддержки](#) и просмотреть информацию о версии продукта и дате последнего обновления компонентов и вирусных баз;
- Кнопка  в верхней части окна — доступ к окну **Лента уведомлений**, где вы можете посмотреть важные уведомления о событиях работы программы.

Режим администратора

Для управления всеми группами настроек необходимо переключить Dr.Web в [режим администратора](#), нажав на замок  в нижней части окна. Когда Dr.Web работает в режиме администратора, замок «открыт» .

В любом режиме есть полный доступ к группе настроек **Инструменты**. Также, не переключая Dr.Web в режим администратора, вы можете включить любой из компонентов защиты и запустить Сканер. Выключение компонентов защиты, управление параметрами компонентов и изменение настроек программы возможны только в режиме администратора.

Статусы защиты

В верхней части окна отображается статус защищенности системы.

- **Компьютер защищен** — все компоненты включены и работают, Самозащита включена, лицензия действует. Отображается зеленым цветом.
- **Компьютер не защищен** — отображается, если какой-либо из компонентов защиты отключен. Отображается красным цветом. Плитка отключенного компонента также выделена красным.
- **Лицензия истекает** — начинает отображаться за 7 дней до окончания действия лицензии. Отображается желтым цветом. Для продления лицензии необходимо перейти в [Менеджер лицензий](#).



8. Обновление программных модулей

Для обновления Dr.Web необходимо иметь доступ к интернету либо к зеркалу обновлений (локальной или сетевой папке), либо к антивирусной сети, в которой хотя бы на одном из компьютеров настроено зеркало обновлений. Настройка источника обновлений и других параметров производится в группе настроек **Общие** → **Обновление**. Подробная инструкция по настройке параметров обновления программы Dr.Web доступна в разделе [Настройки обновления](#).

Проверка актуальности обновлений

Чтобы проверить актуальность компонентов, откройте [меню](#) Dr.Web . В случае актуальности обновлений в меню пункт **Обновление** будет выделен зеленым цветом:

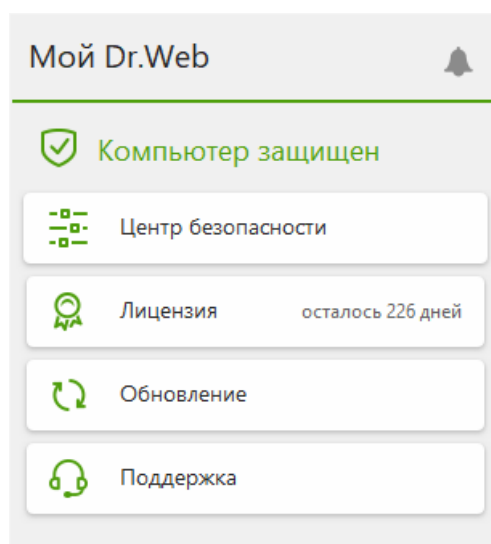


Рисунок 13. Меню Dr.Web

При необходимости обновления в меню появится пункт **Требуется обновление**, выделенный красным цветом:

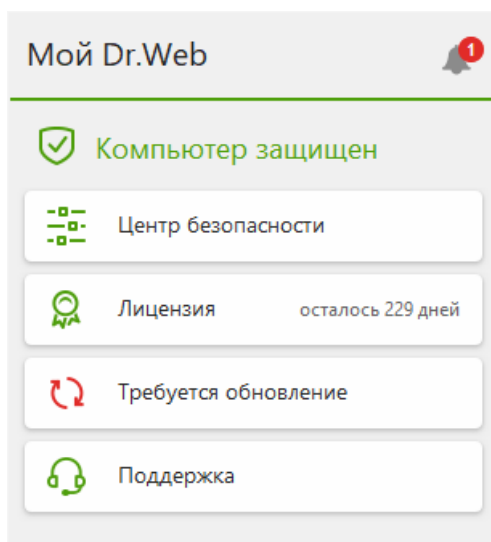


Рисунок 14. Необходимость обновления

Запуск процесса обновления

При обновлении Dr.Web загрузит все обновленные файлы, соответствующие вашей версии Dr.Web, а также новую версию Dr.Web при ее наличии.



При обновлении исполняемых файлов, драйверов и библиотек может потребоваться перезагрузка компьютера. В этом случае будет показано соответствующее предупреждение. Вы можете задать любое удобное время перезагрузки либо выбрать время следующего напоминания.

Чтобы запустить обновления из меню Dr.Web

1. Откройте меню Dr.Web  и выберите пункт **Обновление**. В зависимости от актуальности компонентов цветовая индикация этого пункта может варьироваться.
2. Откроется информация об актуальности обновлений, а также дата последнего обновления. Нажмите кнопку **Обновить**, чтобы запустить процесс обновления.

Чтобы запустить обновления из командной строки

1. Перейдите в папку установки Dr.Web (%PROGRAMFILES%\Common Files\Doctor Web\Updater).
2. Запустите drwupsrv.exe. Список параметров запуска вы можете найти в Приложении А.

Отчеты и журнал статистики

Чтобы посмотреть историю обновлений во вкладке Статистика

1. Откройте меню Dr.Web .



2. Выберите пункт **Центр безопасности**.
3. Перейдите во вкладку **Статистика**.
4. Нажмите плитку **Подробный отчет**.

Отчеты обновления также записываются в файл `dwupdater.log` в папке `%allusersprofile%\Doctor Web\Logs\`.

Как настроить обновление компонентов без доступа к интернету?

Если компьютер подключен к локальной сети, вы можете настроить обновление компонентов с зеркала обновлений, созданного на другом компьютере с установленным продуктом Dr.Web (Security Space, Антивирус для Windows, Katana или Server Security Suite). Компьютер, на котором создано зеркало обновлений, должен быть подключен к интернету. Версия продукта должна совпадать.

[Подробнее о том, как настроить зеркало обновлений](#)

Вы можете настроить обновление с зеркала обновлений двумя способами:

Чтобы настроить получение обновлений при подключении к антивирусной сети

1. Разрешите удаленное управление продуктом Dr.Web в разделе настроек [Антивирусная сеть](#).

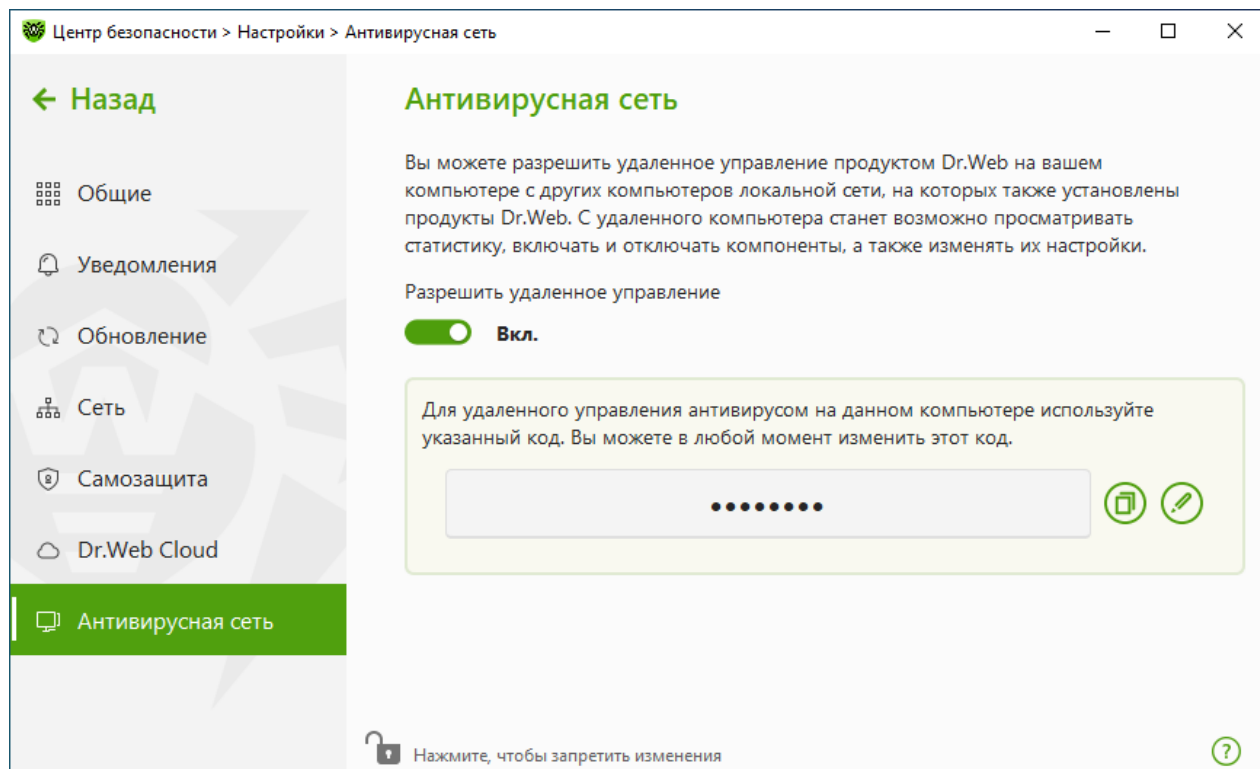


Рисунок 15. Включение удаленного доступа

2. Перейдите в окно **Настройки** → **Обновление**.



3. В пункте **Источник обновлений** нажмите **Изменить** и в выпадающем списке выберите **Антивирусная сеть**.

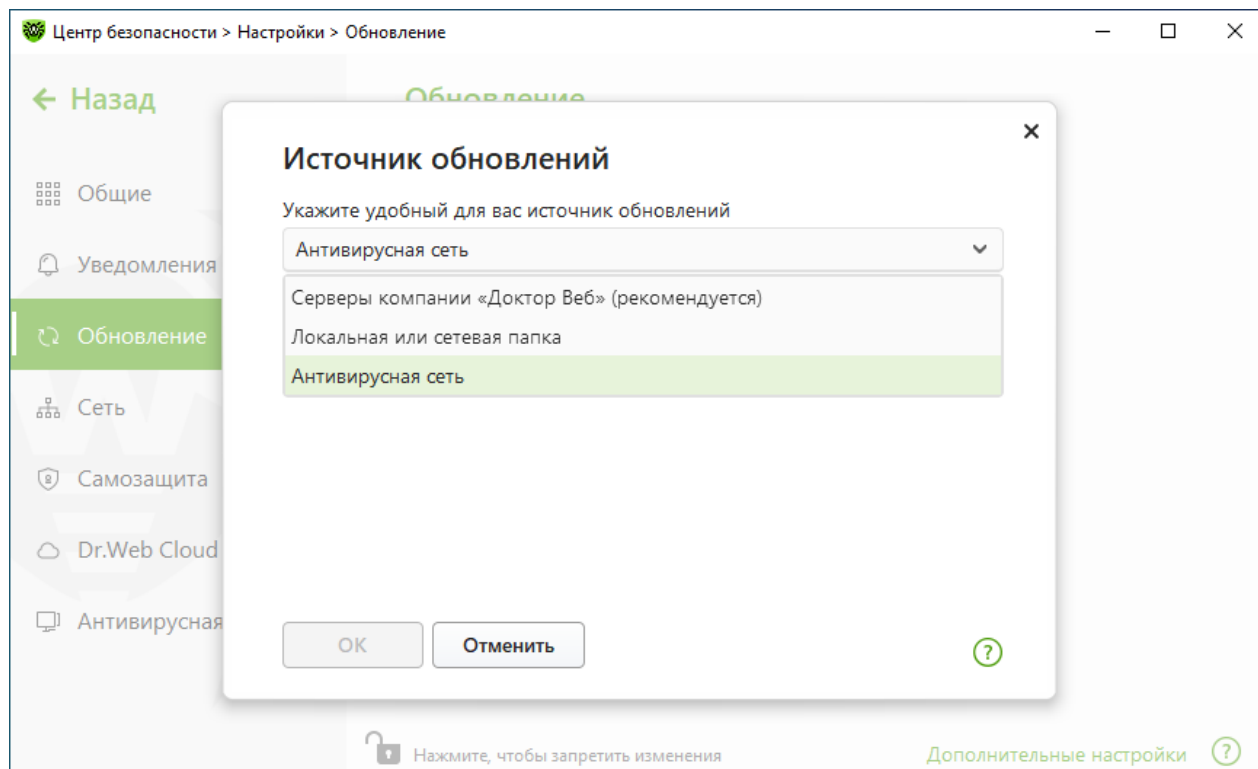


Рисунок 16. Выбор источника обновлений

4. Выберите необходимый компьютер, с которого будет производиться обновление компонентов программы.
5. Нажмите **ОК**.

Чтобы настроить получение обновлений из локальной или сетевой папки

1. Перейдите в окно **Настройки** → **Обновление**.
2. В пункте **Источник обновлений** нажмите **Изменить** и в выпадающем списке выберите **Локальная или сетевая папка**.

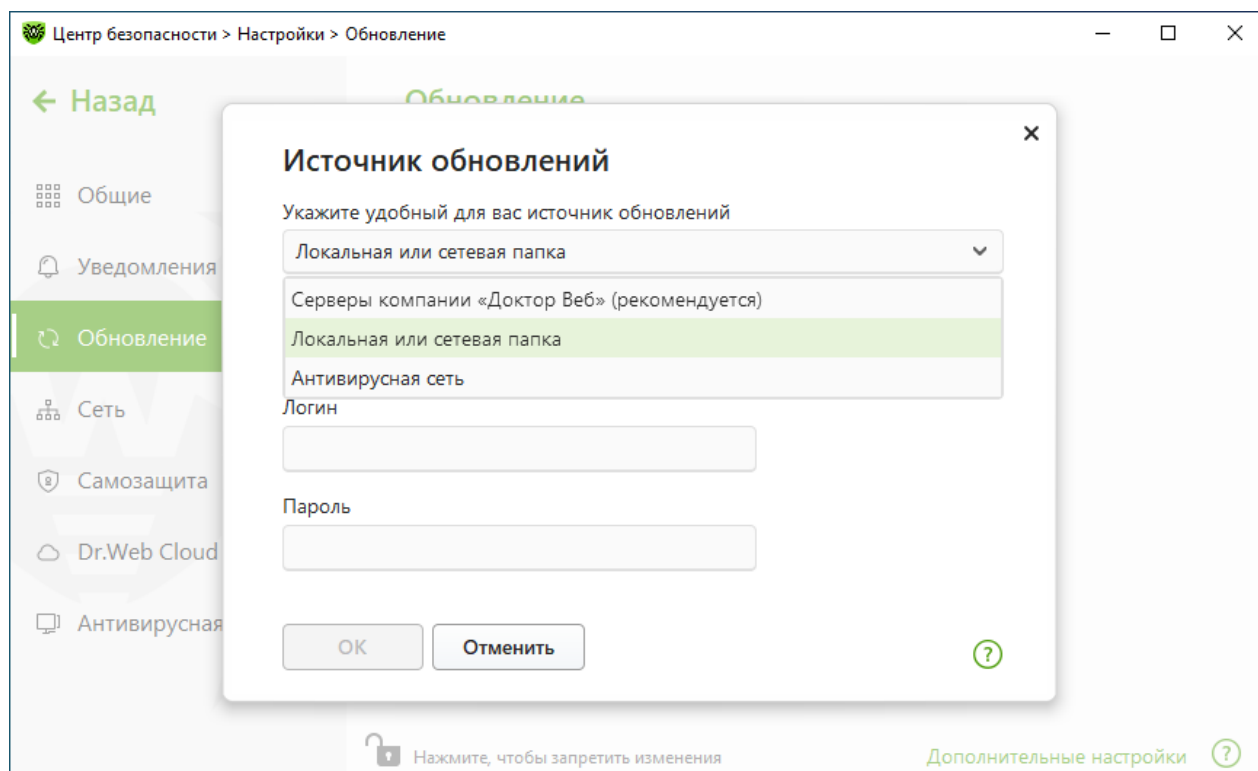


Рисунок 17. Выбор источника обновлений

3. В строке **Путь к зеркалу обновлений** укажите папку, содержащую файлы созданного зеркала обновлений. Для этого нажмите кнопку **Обзор** и выберите нужную папку или введите путь вручную в формате UNC.
4. При необходимости укажите **Логин** и **Пароль** к папке, к которой осуществляется подключение. **Логин** — это имя пользователя учетной записи на компьютере, где лежит сетевая папка. Логин должен включать название компьютера в локальной сети и полный путь к папке. **Пароль** — это пароль этой учетной записи.
5. Нажмите **ОК**.



9. Лента уведомлений

В этом окне собраны важные уведомления о событиях работы программы. Уведомления в этом разделе дублируют некоторые из всплывающих на экране уведомлений.

Чтобы перейти к ленте уведомлений из Меню программы

1. Откройте [меню](#) Dr.Web .
2. Нажмите кнопку . Над значком  отображается количество сохраненных уведомлений.
3. Откроется окно с уведомлениями о событиях.

Чтобы перейти к ленте уведомлений из Центра безопасности

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. В верхней части окна программы нажмите .
3. Откроется окно с уведомлениями о событиях.

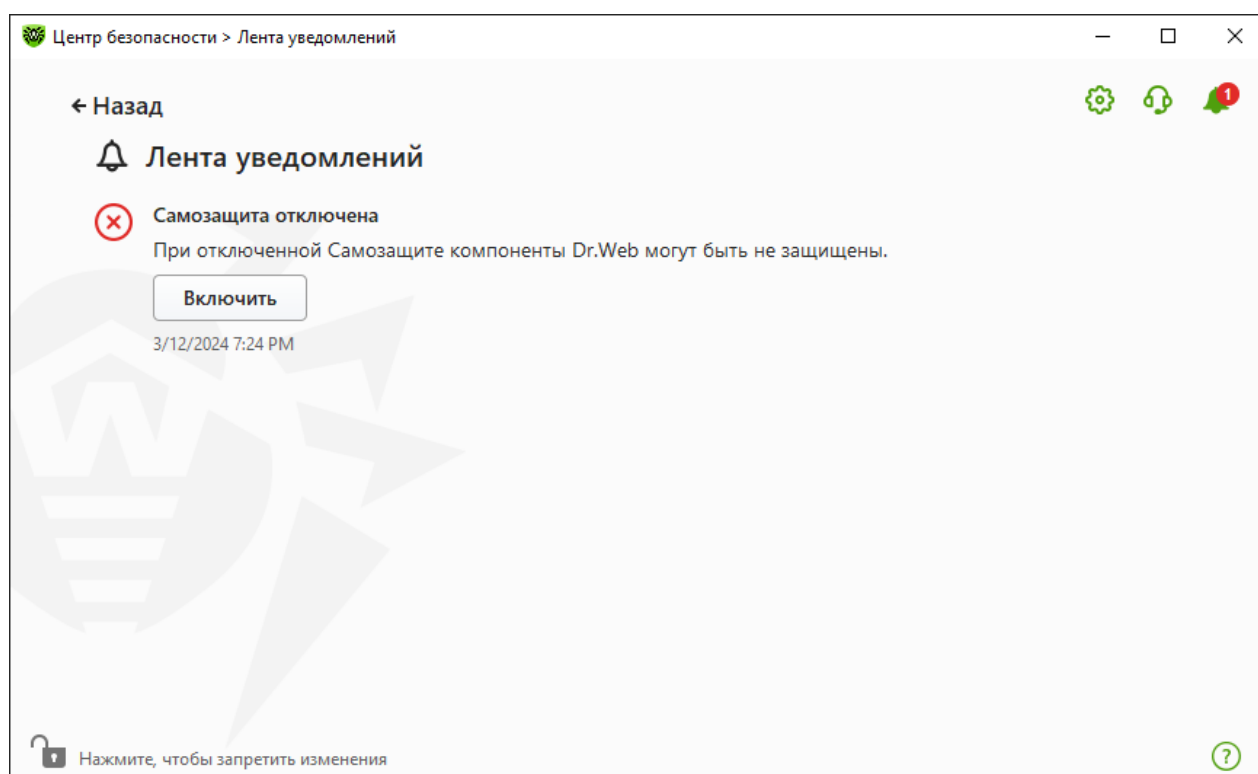


Рисунок 18. Окно ленты уведомлений



Срок хранения уведомлений

Срок хранения уведомлений составляет две недели. При устранении проблем уведомления о них также удаляются.

Типы уведомлений

 Критические уведомления	
Лицензия	• Действующая лицензия не найдена. • Текущая лицензия заблокирована.
Угрозы	• Обнаружена угроза.
 Важные уведомления	
Лицензия	• Срок действия лицензии истекает. • Текущая лицензия заблокирована.
Обновление	• Требуется перезагрузка, чтобы обновления вступили в силу.
Компоненты	• Изменение метода Защиты от потери данных.
 Маловажные информационные уведомления	
Новая версия	• Доступна новая версия продукта.

Настройки отображения

Настройки отображения уведомлений в ленте дублируют настройки всплывающих уведомлений. Если вы хотите изменить настройки отображения так, чтобы определенные уведомления не отображались в ленте, в окне **Параметры уведомлений** необходимо снять флажок в столбце **Экран** напротив необходимого пункта (см. раздел [Настройки уведомлений](#)).



10. Настройки программы

Чтобы перейти к изменению настроек программы

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
3. В верхней части окна программы нажмите .
4. Откроется окно с настройками программы.



Если в [общих настройках](#) вы установили флажок **Защищать настройки Dr.Web паролем**, для доступа к основным настройкам Dr.Web запрашивается пароль.

В этом разделе:

- [Общие](#) — защита настроек паролем, выбор языка программы, выбор цвета темы интерфейса, а также импорт и экспорт настроек.
- [Уведомления](#) — настройка вывода уведомлений на экран или получение их по почте.
- [Обновление](#) — изменение источника или периодичности обновлений и создание зеркала обновлений.
- [Сеть](#) — настройка использования прокси-сервера и проверки данных, передаваемых по безопасным протоколам.
- [Самозащита](#) — настройка дополнительных параметров безопасности.
- [Dr.Web Cloud](#) — настройка доступа к облачным сервисам компании «Доктор Веб».
- [Антивирусная сеть](#) — настройка удаленного доступа к Dr.Web, установленному на вашем компьютере.

10.1. Общие настройки

К общим настройкам относятся следующие:

- [защита настроек программы паролем](#);
- [выбор цвета темы интерфейса](#);
- [выбор языка программы](#);
- [управление настройками программы](#) (импорт, экспорт, восстановление настроек по умолчанию);
- [настройки ведения журнала работы](#);
- [настройки карантина](#);
- [настройки автоматического удаления записей статистики](#).



Чтобы открыть общие настройки

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Общие**.

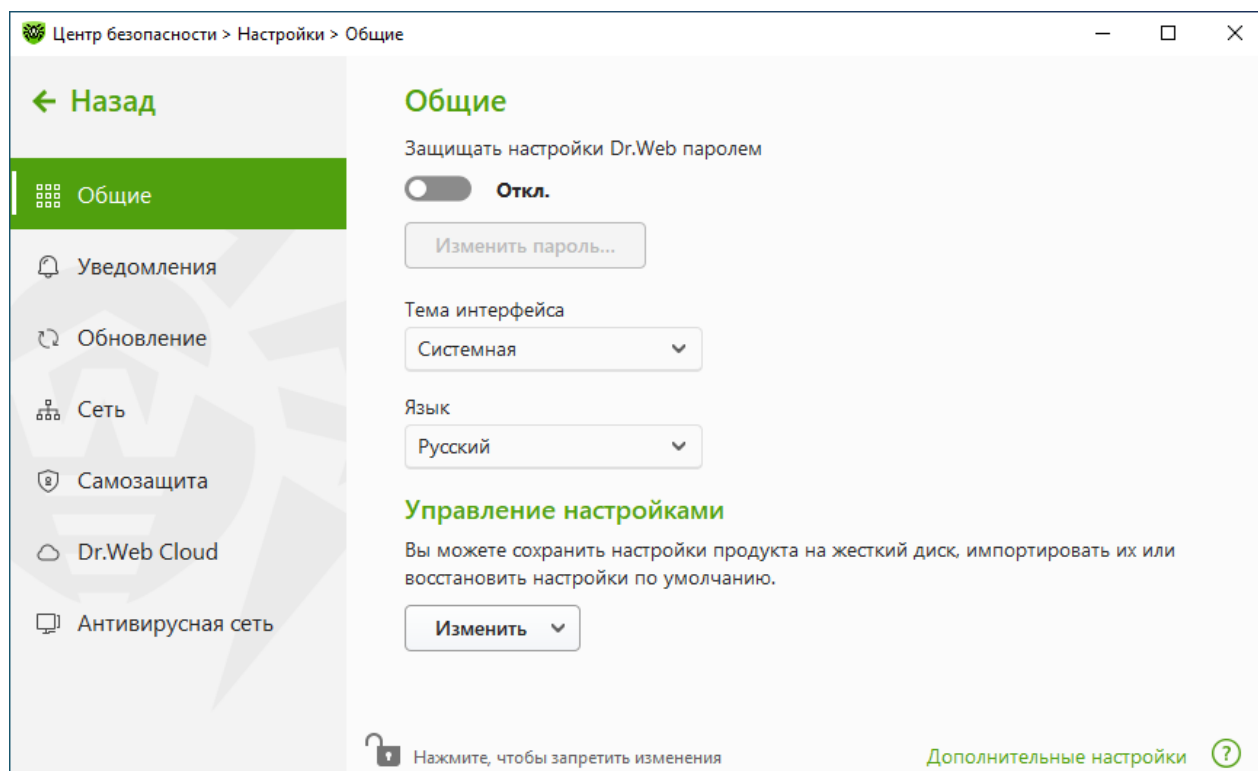


Рисунок 19. Общие настройки

10.1.1. Защита настроек программы паролем

Вы можете ограничить доступ к настройкам Dr.Web на вашем компьютере при помощи пароля. Пароль не ограничен по длине и может включать в себя любую комбинацию букв, цифр и специальных символов. Для более надежной защиты используйте пароль, состоящий из 10 или более различных знаков. Пароль будет запрашиваться каждый раз при обращении к настройкам Dr.Web.

Чтобы задать пароль

1. В окне изменения общих настроек включите опцию **Защищать настройки Dr.Web паролем** при помощи соответствующего переключателя .

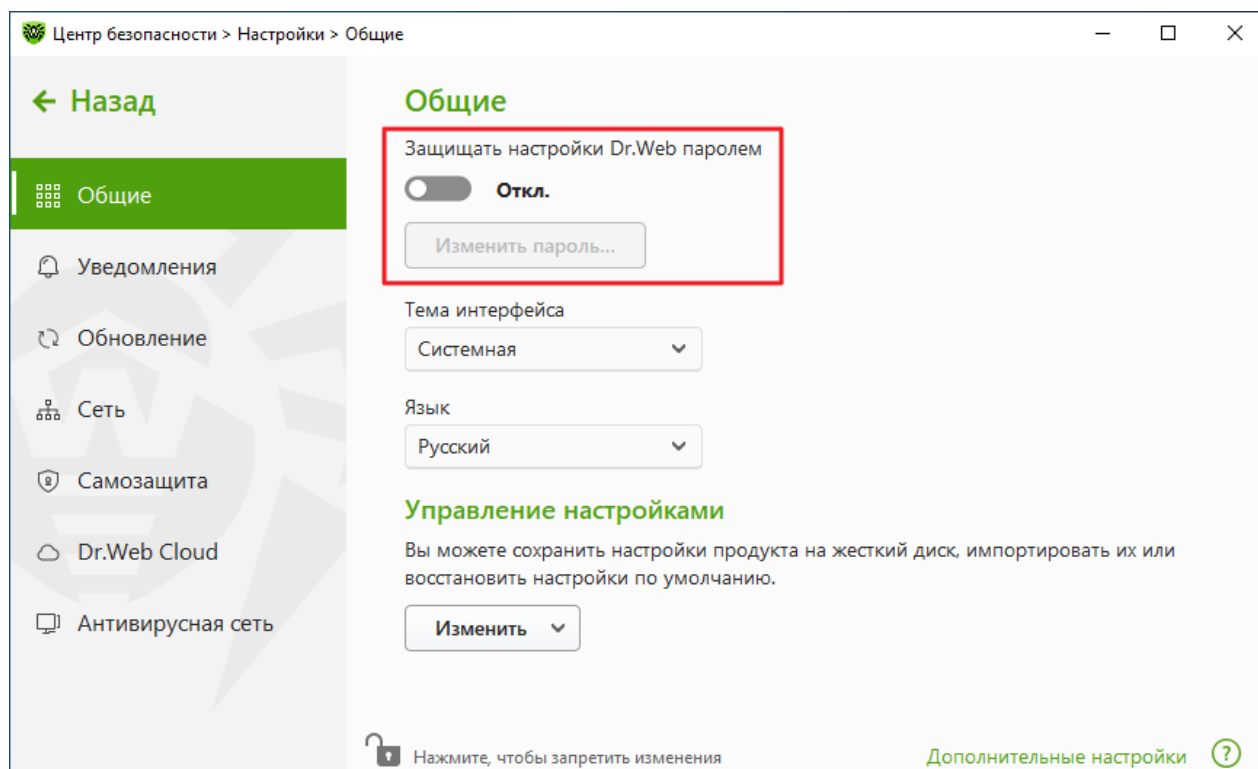


Рисунок 20. Защита настроек паролем

2. В открывшемся окне задайте пароль и подтвердите его ввод.
3. Нажмите кнопку **ОК**.



Если вы забыли пароль к настройкам продукта, необходимо переустановить программу Dr.Web без сохранения текущих настроек.

10.1.2. Выбор цвета темы интерфейса

При необходимости вы можете изменить цвет темы интерфейса программы. Для этого в выпадающем списке **Тема интерфейса** выберите одну из опций:

- **Светлая**, чтобы использовать светлое оформление программы.
- **Темная**, чтобы использовать темное оформление программы.
- **Системная**, чтобы использовать цвет интерфейса, соответствующий теме, выбранной в операционной системе. Эта опция выбрана по умолчанию.

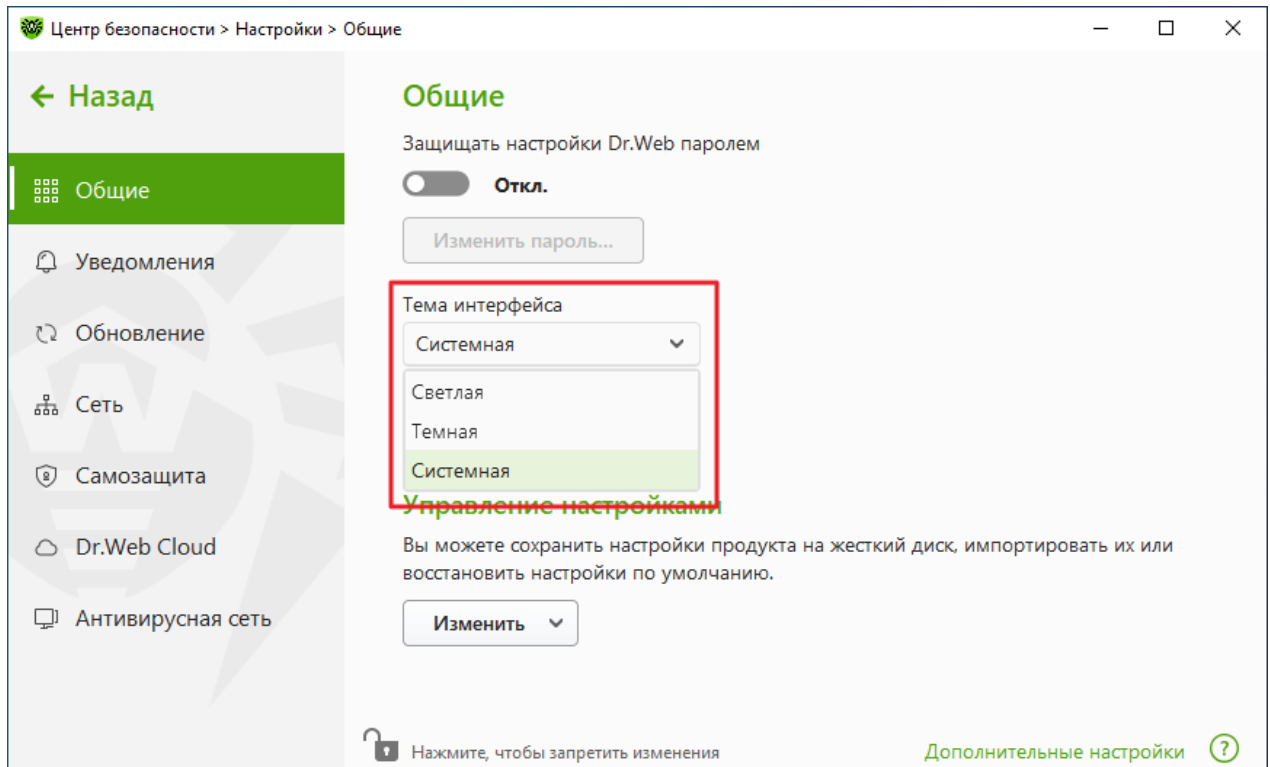


Рисунок 21. Выбор цвета темы интерфейса



Темная тема доступна только на компьютерах с операционной системой Windows 10 (начиная с версии 1909), Windows 11 и Windows Server 2019 (начиная с версии 1809) и более поздних. Настройки выбора цвета темы интерфейса скрыты для более ранних версий операционной системы.



10.1.3. Выбор языка программы

При необходимости вы можете переключить язык интерфейса программы. Список языков пополняется автоматически и содержит все доступные на текущий момент локализации графического интерфейса Dr.Web. Для этого в выпадающем списке **Язык** выберите необходимый язык.

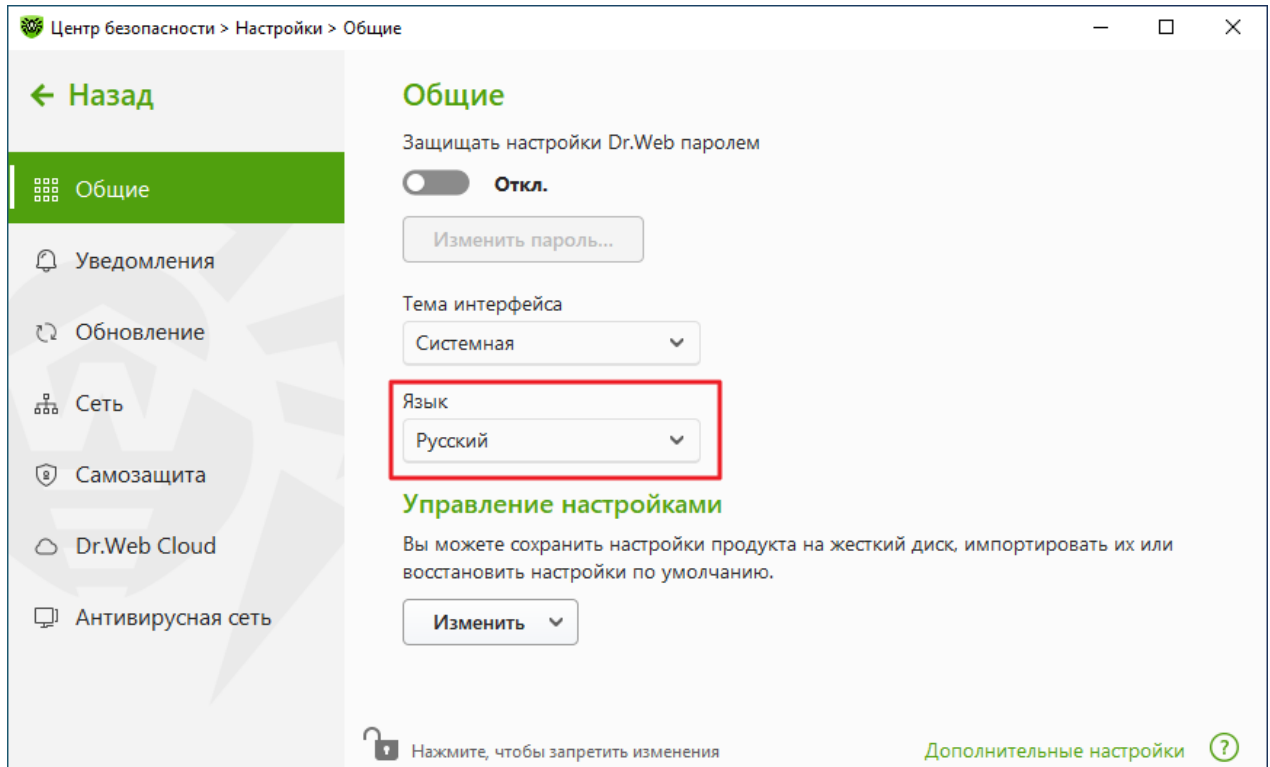


Рисунок 22. Выбор языка программы



10.1.4. Управление настройками Dr.Web

Для управления настройками выберите одно из следующих значений в выпадающем списке группы настроек **Управление настройками**:

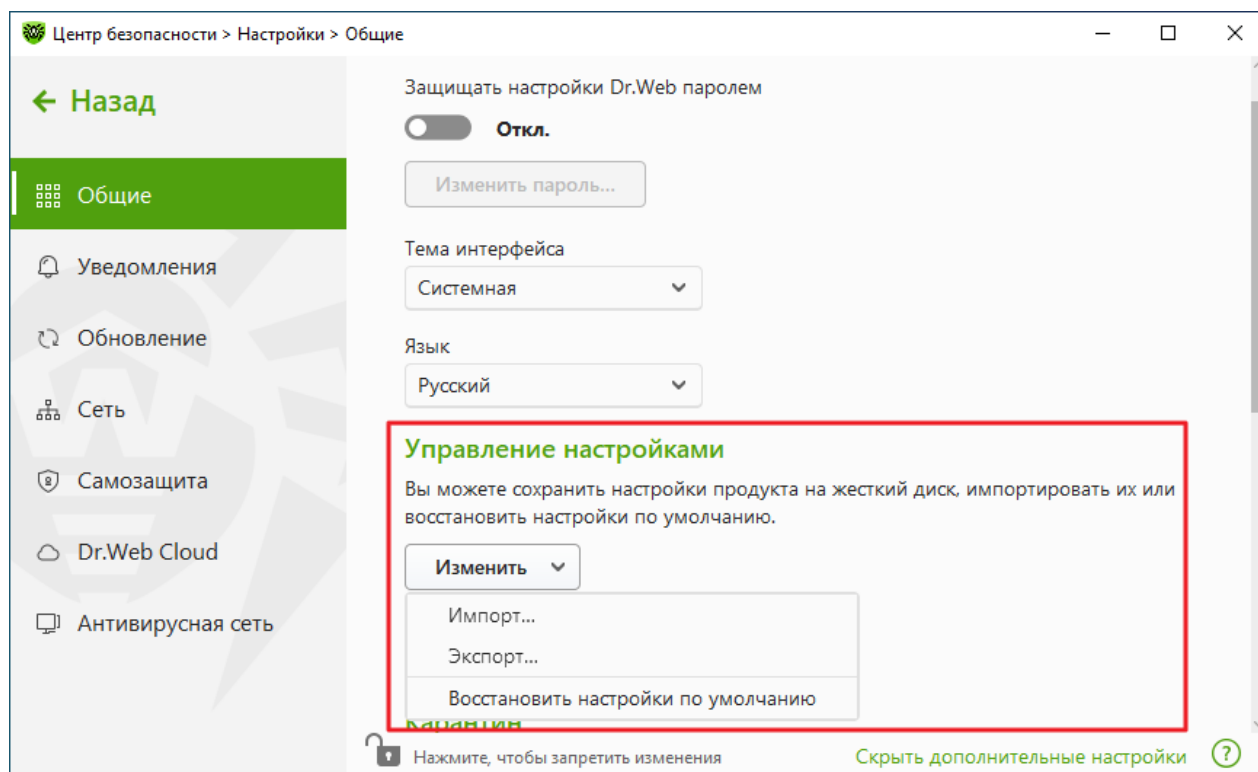


Рисунок 23. Управление настройками

- **Восстановить настройки по умолчанию**, чтобы сбросить пользовательские настройки до настроек по умолчанию.
- **Импорт**, если вы уже настроили работу антивируса на другом компьютере и хотите использовать те же настройки.
- **Экспорт**, если вы хотите использовать свои настройки на других компьютерах. Затем воспользуйтесь функцией импорта настроек на другом компьютере.

10.1.5. Ведение журнала работы Dr.Web

Вы можете включить ведение подробного журнала о работе одного или нескольких компонентов или служб Dr.Web.

Чтобы изменить настройки ведения журнала

1. Нажмите ссылку **Дополнительные настройки**.
2. В разделе настроек **Журнал** нажмите кнопку **Изменить**.

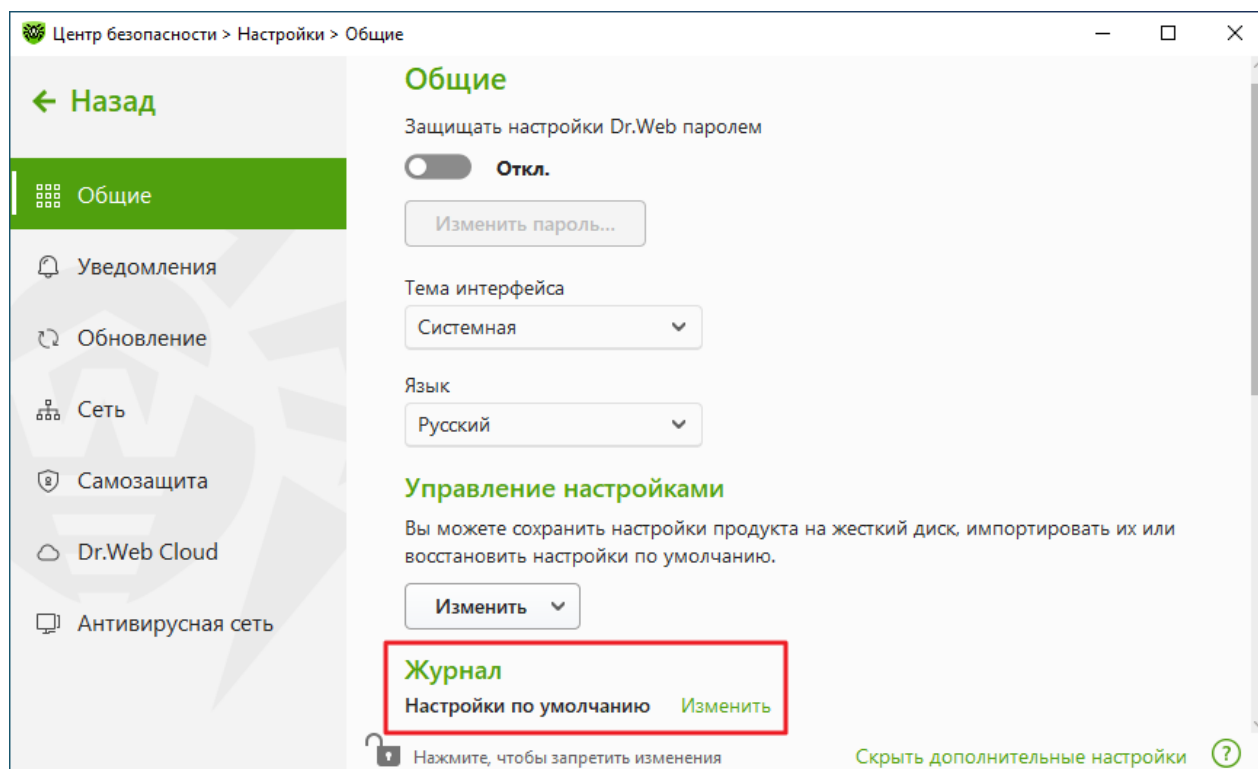


Рисунок 24. Общие настройки. Журнал

Откроется окно настроек ведения подробного журнала:

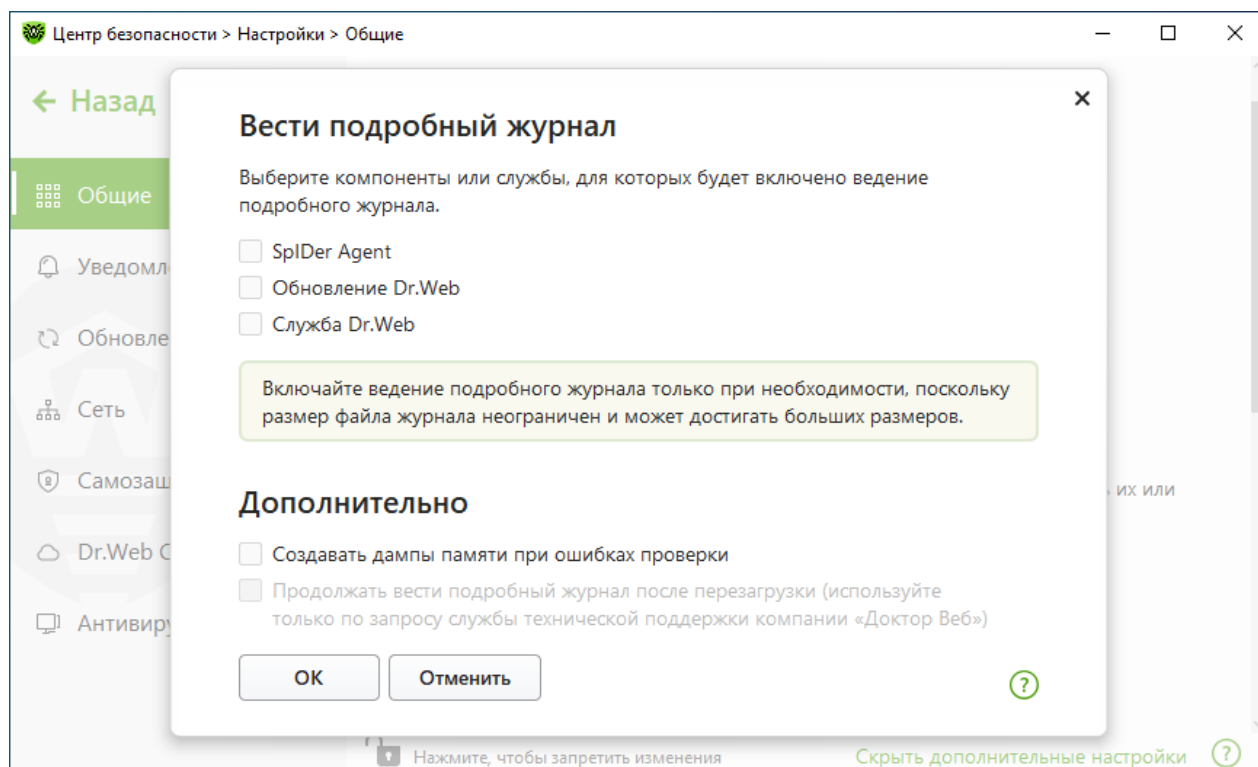


Рисунок 25. Настройки ведения журнала работы

3. Выберите компоненты, модули или службы, для которых будет включено ведение подробного журнала. По умолчанию для всех компонентов Dr.Web журнал ведется в стандартном режиме, фиксирующем следующую информацию:



Компонент	Информация
SplDer Agent	Проведение обновлений, запуск и остановка SplDer Agent, обнаруженные угрозы, соединение с антивирусной сетью, лицензионные события, состояние работы компонентов Dr.Web, управление настройками (импорт, экспорт), уведомления об ошибках, уведомления о перезагрузке системы. Рекомендуется использовать этот режим для получения детальной информации об источниках ошибок в работе программы.
Обновление Dr.Web	Список обновленных файлов Dr.Web и статусы их загрузки, информация о работе вспомогательных скриптов, дата и время проведения обновления, информация о перезапуске компонентов Dr.Web после обновления.
Служба Dr.Web	Информация о компонентах Dr.Web, изменение настроек компонентов, включение и выключение компонентов, события превентивной защиты, подключение к антивирусной сети.

Создание дампов памяти

Настройка **Создавать дампы памяти при ошибках проверки** позволяет сохранять полезную информацию о работе некоторых компонентов Dr.Web, что даст возможность специалистам компании «Доктор Веб» в дальнейшем провести более полный анализ проблемы и предложить ее решение. Рекомендуется включать данную настройку по просьбе сотрудников технической поддержки компании «Доктор Веб» или при возникновении ошибок проверки файлов или обезвреживания угроз. Дамп памяти сохраняется в виде файла с расширением `.dmp` в папке `%PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\`.

Включение подробных журналов



При включении подробных журналов фиксируется максимальное количество информации о работе компонентов Dr.Web. Это приведет к отключению ограничения на размер файлов журнала и снизит производительность работы Dr.Web и операционной системы. Использовать этот режим следует только при возникновении проблем в работе компонентов или по просьбе службы технической поддержки компании «Доктор Веб».

1. Чтобы включить режим ведения подробного журнала для одного из компонентов Dr.Web, установите соответствующий флажок.
2. По умолчанию подробный журнал ведется до первой перезагрузки операционной системы. Если необходимо зафиксировать поведение компонента в период до и после перезагрузки, установите флажок **Продолжать вести подробный журнал после перезагрузки (используйте только по запросу службы технической поддержки компании «Доктор Веб»)**.
3. Сохраните изменения, нажав кнопку **ОК**.



По умолчанию файлы журнала имеют ограниченный размер, равный 10 МБ. При превышении максимального размера файл журнала урезается до:

- заданного размера, если информация, записанная за сессию, не превышает разрешенный размер;
- размера текущей сессии, если информация, записанная за сессию, превышает разрешенный размер.

10.1.6. Настройки карантина

Чтобы чрезмерно не загружать диск, вы можете задать настройки хранения объектов в карантине, такие как время хранения объектов и создание папки карантина на съемном носителе.

Чтобы изменить настройки хранения обнаруженных угроз

1. В окне изменения общих настроек нажмите ссылку **Дополнительные настройки**.
2. В разделе настроек **Карантин** включите или отключите необходимую опцию при помощи переключателя .

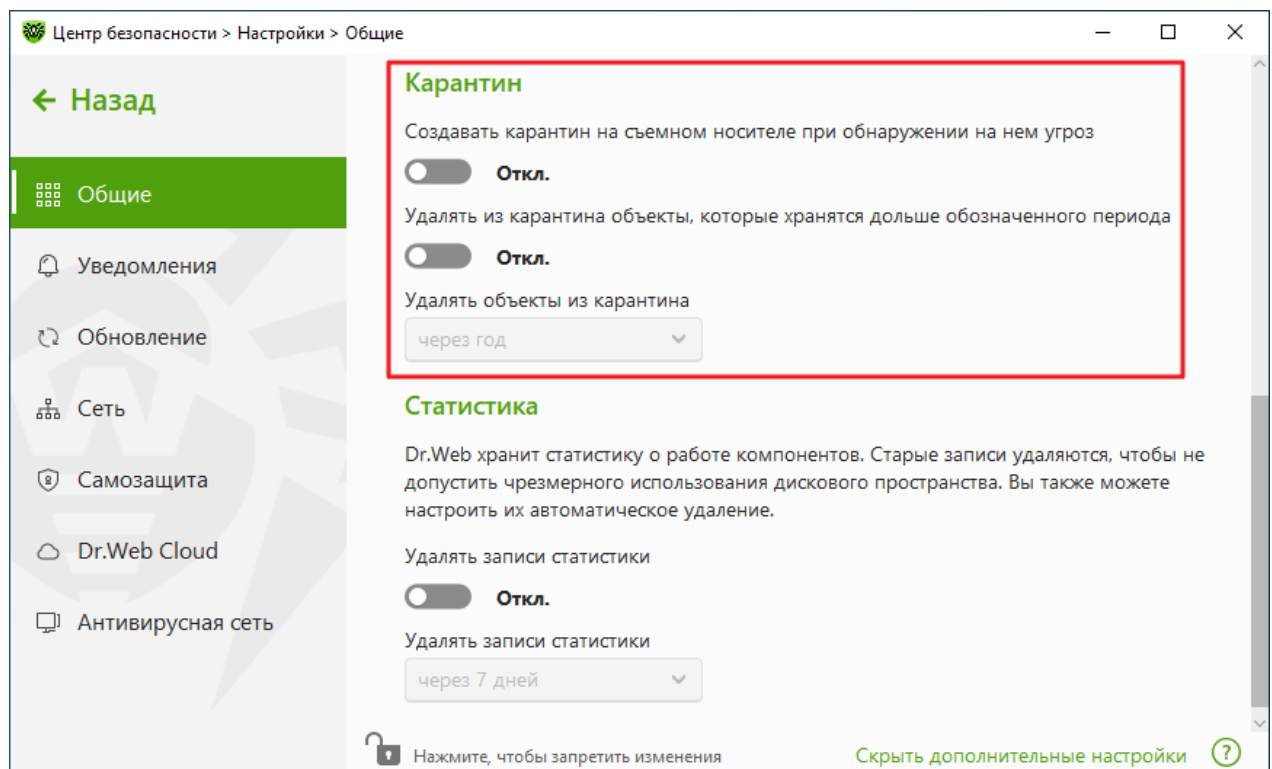


Рисунок 26. Настройки карантина

3. При включении автоматического удаления объектов из карантина в выпадающем меню выберите время. Объекты, хранящиеся дольше указанного срока, будут удаляться.



Создание карантина на съемном носителе

Опция **Создавать карантин на съемном носителе при обнаружении на нем угроз** позволяет при обнаружении угрозы на съемном носителе создавать папку карантина на том же носителе и помещать в эту папку угрозы без предварительного шифрования. На съемном носителе папка карантина создается, только если возможна запись на носитель. Использование отдельных папок и отказ от шифрования на съемных носителях позволяет предотвратить возможную потерю данных.

Если опция отключена, обнаруженные на съемных носителях угрозы помещаются в карантин на локальном диске.

Автоматическое удаление объектов из карантина

Чтобы избежать чрезмерного использования места на диске, включите автоматическое удаление объектов из карантина.

10.1.7. Автоматическое удаление записей статистики

По умолчанию Dr.Web хранит оптимальное количество записей [статистики](#), чтобы избежать чрезмерного использования места на диске. В дополнение к этому вы можете включить автоматическое удаление записей, хранящихся дольше указанного срока.

Чтобы включить или отключить автоматическое удаление записей статистики

1. В окне изменения общих настроек нажмите ссылку **Дополнительные настройки**.
2. В разделе настроек **Статистика** включите или отключите автоудаление записей статистики при помощи переключателя .

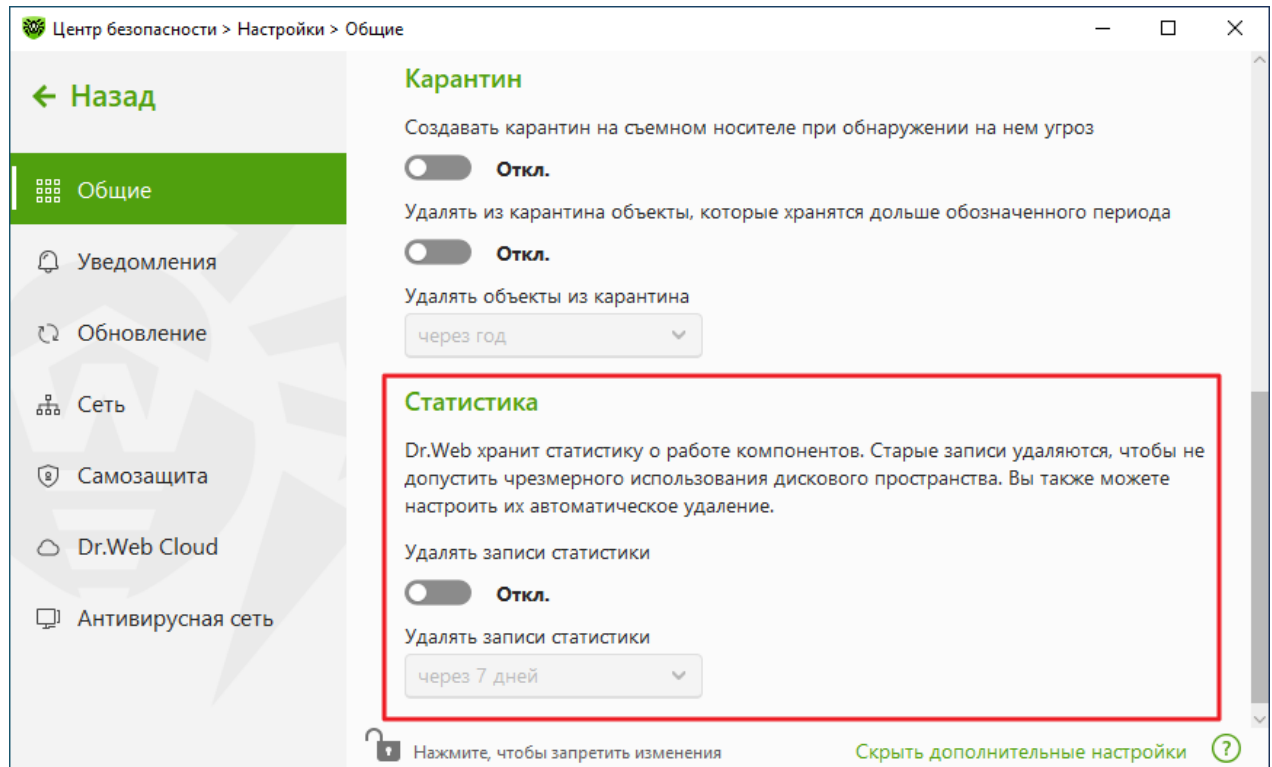


Рисунок 27. Настройки статистики

3. При включении автоудаления записей статистики в выпадающем меню выберите время. Записи, хранящиеся дольше указанного срока, будут удаляться.

10.2. Настройки уведомлений

Вы можете настроить параметры получения уведомлений о критичных и важных событиях работы Dr.Web.

В этом разделе:

- [Настройка параметров уведомлений](#)
- [Настройка вывода уведомлений на экран](#)
- [Настройка отправки уведомлений по почте](#)

При необходимости настройте параметры получения уведомлений о критичных и важных событиях работы Dr.Web.

Чтобы открыть настройки уведомлений

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
3. В верхней части окна программы нажмите .



4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Уведомления**.

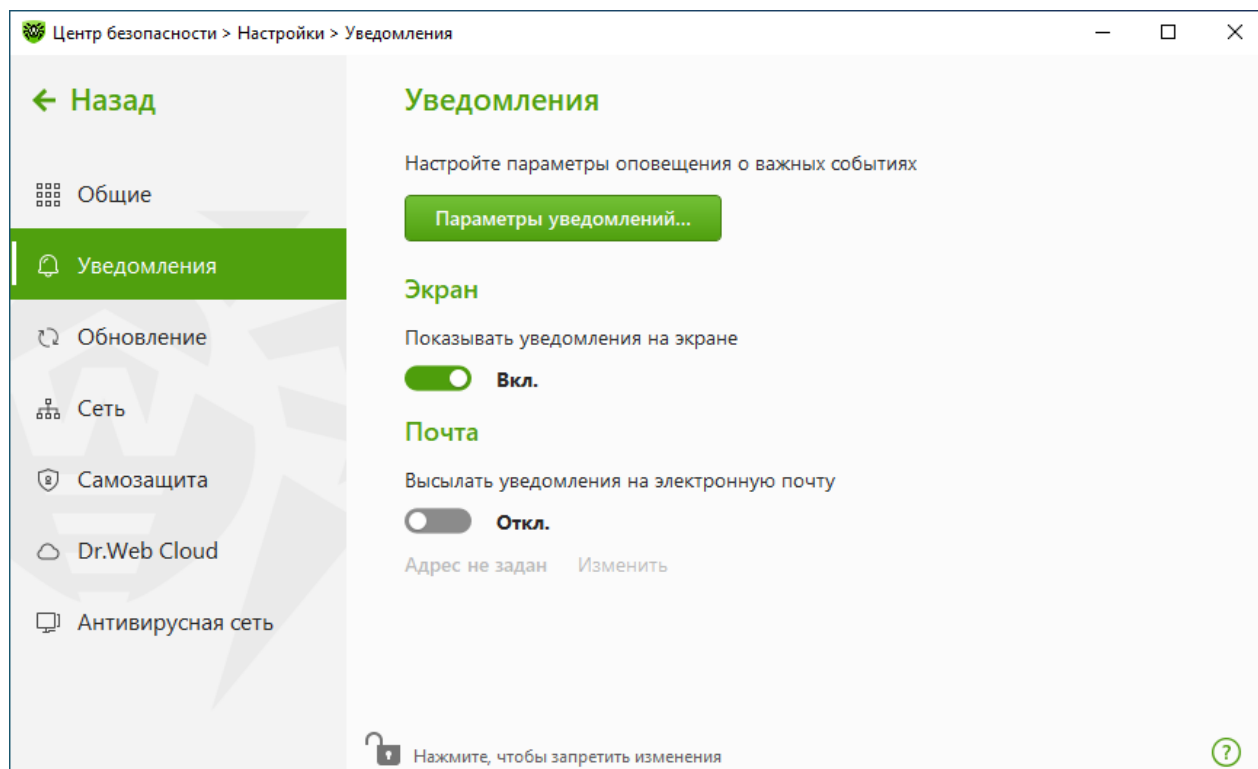


Рисунок 28. Настройки уведомлений

Чтобы настроить параметры уведомлений

1. Нажмите кнопку **Параметры уведомлений**.
2. Выберите уведомления, которые вы хотите получать.
 - Чтобы уведомления отображались на экране, установите соответствующий флажок в столбце **Экран**.
 - Чтобы получать оповещения по почте, установите соответствующий флажок в столбце **Почта**.

Если вы не хотите получать уведомления о событии, снимите флажки.

Тип уведомления	Описание
Важные уведомления	Важные уведомления о следующих событиях: • Заблокирована попытка изменения системных даты и времени. • Доступ к защищаемому объекту заблокирован Поведенческим анализом. • Доступ к защищаемому объекту заблокирован Защитой от эксплойтов. • Доступ к защищаемому объекту заблокирован Защитой от вымогателей.



Тип уведомления	Описание
	• Информация об обновлениях и поддержке продукта. По умолчанию уведомления включены.
Малозначительные уведомления	Малозначительные уведомления о следующих событиях: • Успешное обновление. • Ошибка обновления. • Процессу запрещено изменение содержимого папки. По умолчанию уведомления выключены, кроме уведомления о запрещении процессу изменения содержимого папки.
Лицензия	Уведомления о следующих событиях: • Срок действия лицензии истекает. • Действующая лицензия не найдена. • Текущая лицензия заблокирована.

3. При необходимости задайте дополнительные параметры отображения экранных оповещений:

Флажок	Описание
Не показывать уведомления в полноэкранном режиме	Отображение уведомлений при работе с приложениями в полноэкранном режиме (просмотр фильмов, графики и т. д.). Снимите этот флажок, чтобы получать уведомления всегда.

4. Если вы выбрали одно или несколько почтовых уведомлений, настройте [отправку почты](#) с вашего компьютера.



Уведомления о некоторых событиях не входят в перечисленные группы и всегда показываются пользователю:

- установка приоритетных обновлений, для которых требуется перезагрузка;
- перезагрузка для завершения обезвреживания угроз;
- автоматическая перезагрузка;
- запрос на разрешение процессу модификации объекта;
- активирована пробная версия, рекомендуется приобрести лицензию.

Уведомления, которые выводятся на экран

В окне настроек уведомлений включите соответствующую опцию, чтобы получать уведомления в виде всплывающего окна над значком Dr.Web  в области уведомлений Windows.



Уведомления по почте

Чтобы получать уведомления о событиях по почте

1. В окне настроек уведомлений включите опцию **Высылать уведомления на электронную почту**.
2. В появившемся окне введите адрес электронной почты, на который вы хотите получать уведомления. Использование этого адреса необходимо будет подтвердить на [шаге 7](#).

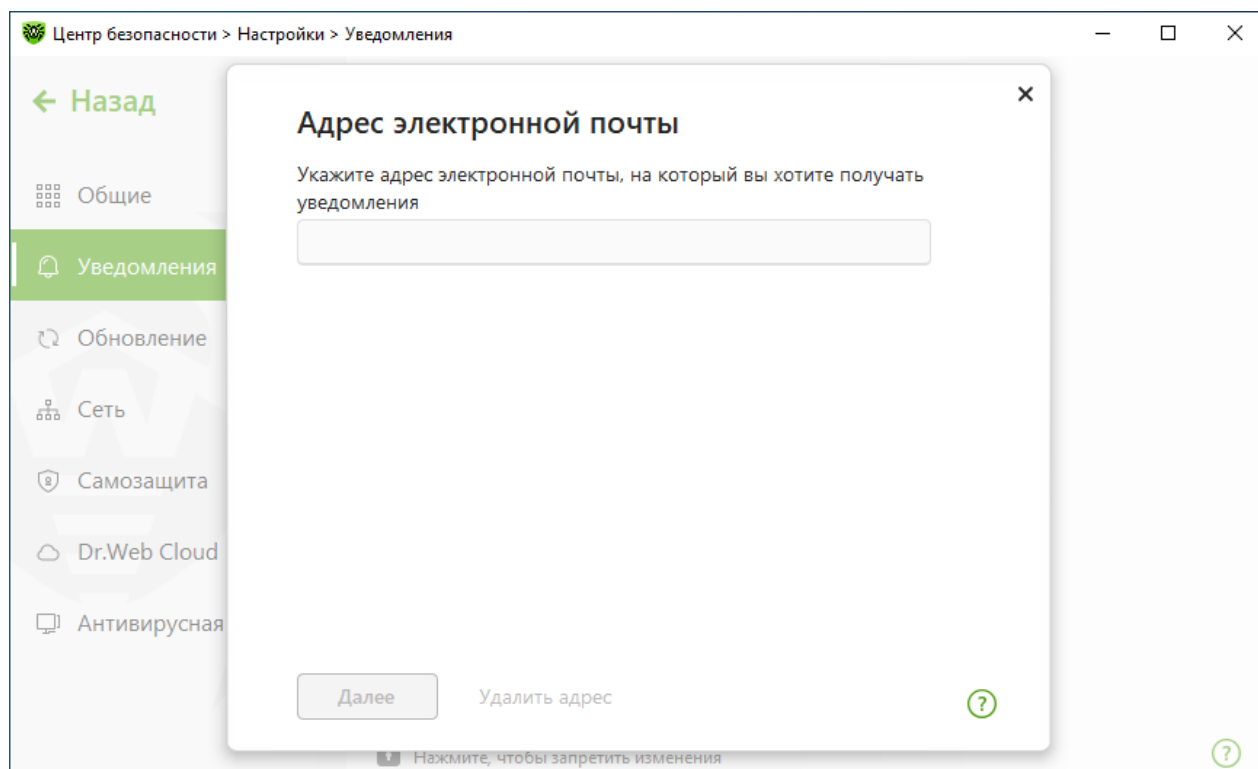


Рисунок 29. Указание адреса для почтовых уведомлений

3. Нажмите **Далее**.
4. В открывшемся окне укажите данные учетной записи, с которой будут отправляться уведомления.
 - Если список почтовых серверов содержит необходимый сервер, выберите его, а затем укажите логин и пароль от вашей учетной записи.
 - Если список почтовых серверов не содержит необходимого сервера, выберите **Указать вручную** и в открывшемся окне заполните необходимые поля:

Настройка	Описание
Сервер SMTP	Укажите адрес почтового сервера, который должен использовать Dr.Web для отправки почтовых оповещений.



Настройка	Описание
Порт	Укажите порт почтового сервера, к которому должен подключаться Dr.Web для отправки почтовых оповещений.
Логин	Укажите имя учетной записи для подключения к почтовому серверу.
Пароль	Укажите пароль учетной записи для подключения к почтовому серверу.
Использовать SSL/TLS	Установите этот флажок, чтобы при передаче сообщений использовалось SSL/TLS шифрование.
NTLM-аутентификация	Установите этот флажок, чтобы авторизация производилась по протоколу NTLM.

5. Нажмите ссылку **Отправить тестовое сообщение**, чтобы проверить, что учетная запись указана верно. Сообщение придет на тот адрес, с которого должны отправляться уведомления (настроенный на [шаге 4](#)).
6. Нажмите **Далее**.
7. Введите код подтверждения, который придет на электронный адрес, указанный для получения уведомлений на [шаге 2](#). Если код не придет в течение 10 минут, нажмите кнопку **Отправить код повторно**. Если вы не введете код подтверждения, уведомления на этот адрес отправляться не будут.

Чтобы изменить адрес электронной почты и другие параметры, в окне настроек уведомлений (см. рисунок [Настройки уведомлений](#)) нажмите **Изменить** и повторите все действия, начиная с [шага 2](#).

10.3. Настройки обновления

Настройте период получения обновлений и источник обновлений для вирусных баз и компонентов. Также вы можете создать зеркало обновлений для получения обновлений на другом компьютере.

Вы можете настроить следующие параметры обновления Dr.Web:

- [периодичность обновлений](#);
- [источник обновлений](#);
- [зеркало обновлений](#).

Чтобы открыть настройки обновления

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .



3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Обновление**.

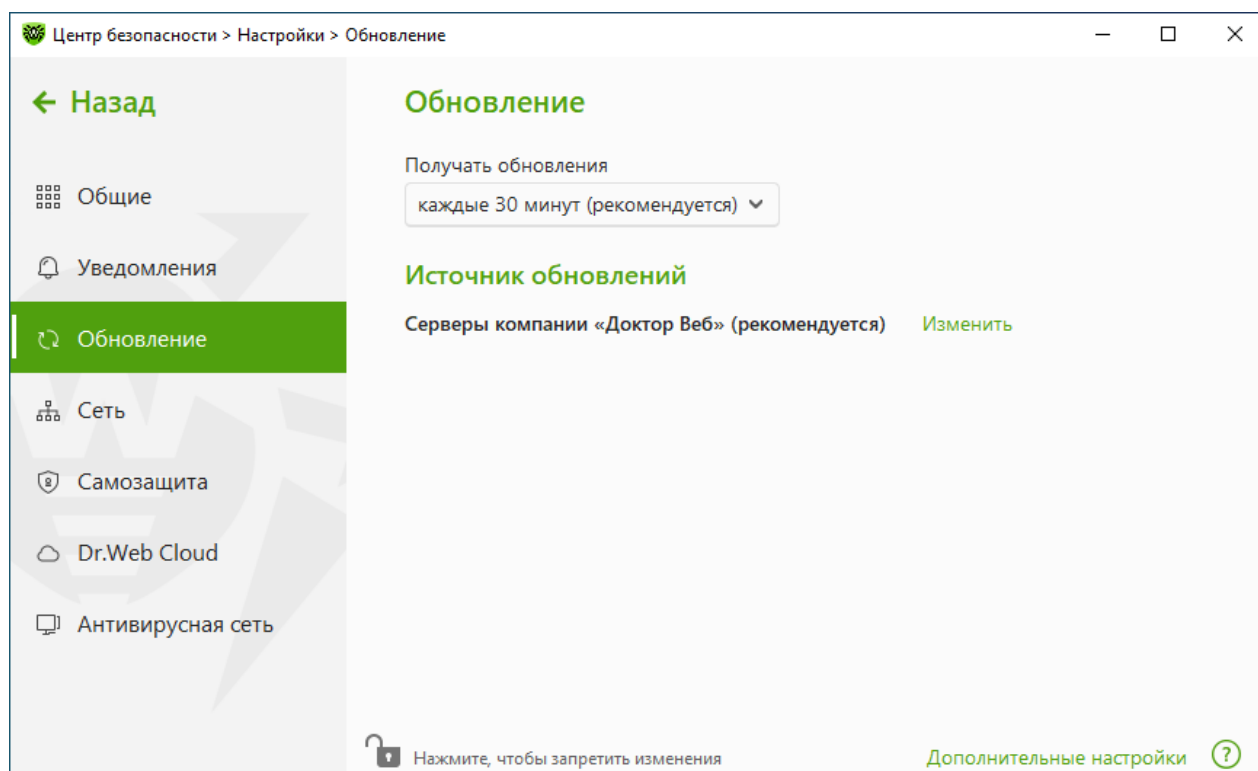


Рисунок 30. Настройки обновления

Периодичность обновлений

По умолчанию установлено оптимальное значение (30 минут), которое позволяет поддерживать информацию об угрозах в актуальном состоянии. Чтобы изменить периодичность обновлений, выберите необходимое значение в выпадающем меню.

Автоматическое обновление проводится в фоновом режиме. Вы также можете выбрать из выпадающего списка значение **Вручную**. В этом случае вам необходимо будет [вручную запускать](#) обновление Dr.Web.

Настройка источника обновлений

По умолчанию в качестве источника обновления указано значение **Серверы компании «Доктор Веб» (рекомендуется)**.

Чтобы настроить удобный для вас источник обновлений

1. В окне настройки обновления (см. рисунок [Настройки обновления](#)) в разделе **Источник обновлений** нажмите ссылку **Изменить**. Откроется окно настройки источника обновлений.

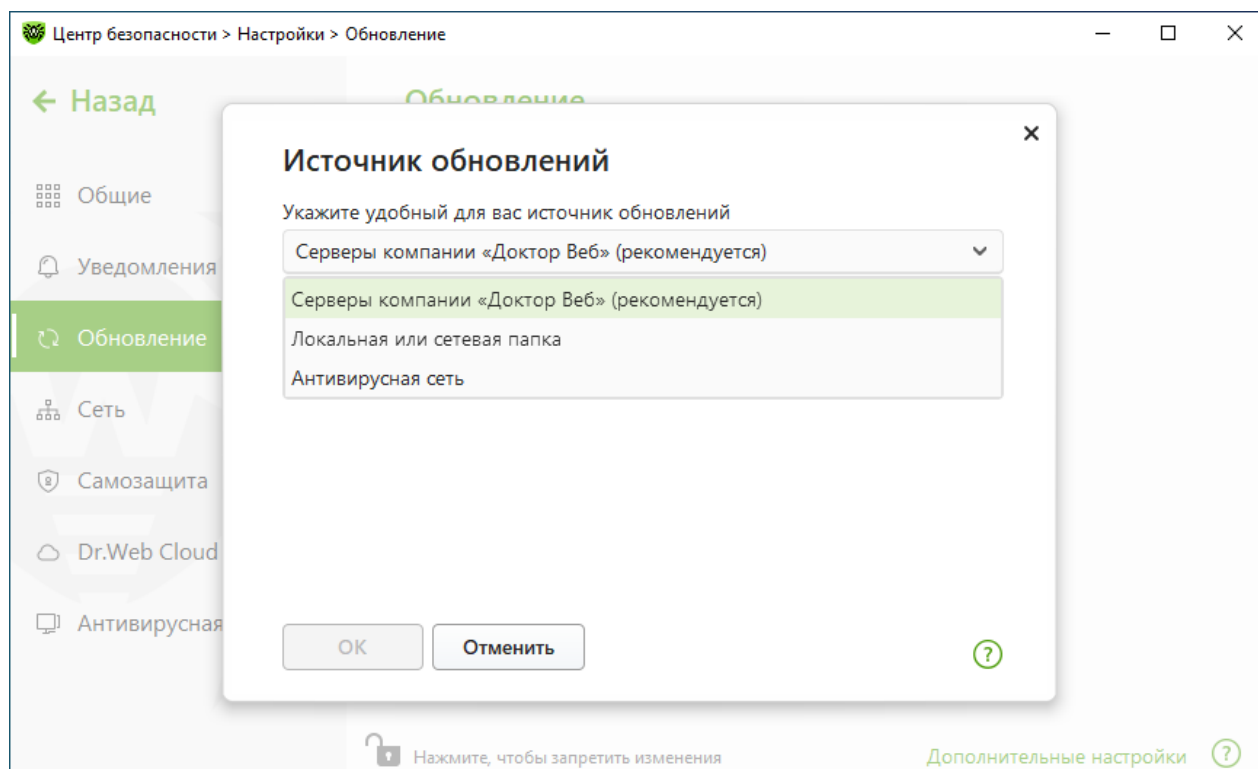


Рисунок 31. Настройка источника обновлений

2. Выберите удобный для вас источник обновлений из выпадающего списка.
 - **Серверы компании «Доктор Веб» (рекомендуется).** Обновление будет происходить с серверов компании «Доктор Веб» через интернет. Если вы хотите загружать обновления по безопасному протоколу при такой возможности, включите опцию **Использовать HTTPS-соединение, когда это возможно**.
 - **Локальная или сетевая папка.** Обновление будет происходить из локальной или сетевой папки, в которую скопированы обновления. Укажите путь к папке (нажав кнопку **Обзор** или введя путь вручную в формате UNC), а также имя пользователя и пароль, если это необходимо.
 - **Антивирусная сеть.** Обновление будет происходить через локальную сеть с компьютера, на котором установлен продукт Dr.Web и создано зеркало обновлений. Выберите компьютер, который будет использоваться в качестве источника обновлений.
3. Нажмите **ОК**, чтобы сохранить изменения.



Если на компьютере уже установлен продукт Dr.Web версии 2.0, не допускается в качестве источника обновлений указывать компьютер с более ранней версией продукта, поскольку это приведет к критическим ошибкам в работе системы.



Дополнительные настройки

Для перехода к дополнительным настройкам в окне **Обновление** (см. рисунок [Настройки обновления](#)) нажмите ссылку **Дополнительные настройки**.

Создание зеркала обновлений

Зеркало обновлений — это папка, в которую копируются обновления. Зеркало обновлений может быть использовано как источник обновлений Dr.Web для компьютеров в локальной сети, которые не подключены к интернету.

Чтобы настроить ваш компьютер в качестве зеркала обновлений

1. В окне настройки обновления (см. рисунок [Настройки обновления](#)) нажмите ссылку **Дополнительные настройки** и включите использование зеркала обновлений при помощи переключателя . Откроется окно настройки зеркала обновлений.

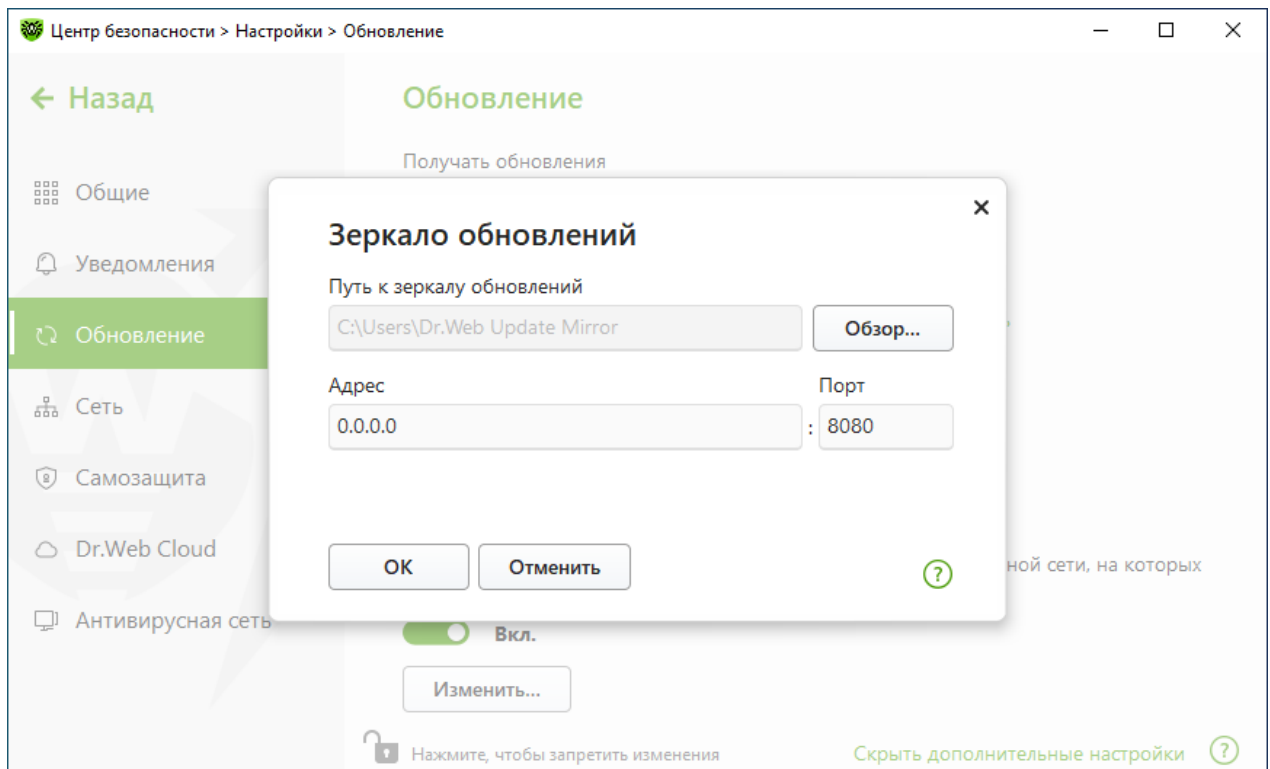


Рисунок 32. Настройка зеркала обновлений

2. Нажмите **Обзор** и выберите папку, в которую будут копироваться обновления. Рекомендуется выбрать пустую папку или создать новую папку. Если указана непустая папка, все ее содержимое будет удалено. Также вы можете указать путь к папке вручную в формате UNC.
3. Если ваш компьютер входит в несколько подсетей, вы можете указать адрес, который будет доступен только для одной из подсетей. Также вы можете указать порт, на котором HTTP-сервер будет принимать запросы на соединение.



- В поле **Адрес** указывается имя хоста или IP-адрес в форматах IPv4 или IPv6.
- В поле **Порт** указывается любой свободный порт.

4. Нажмите **ОК**, чтобы сохранить изменения.

Периодичность загрузки обновлений на зеркало будет совпадать с выбранным значением выпадающего меню **Получать обновления**.

10.4. Сеть

Вы можете настроить параметры соединения с прокси-сервером, включить проверку данных, передаваемых по криптографическим протоколам, а также экспортировать сертификат Dr.Web для последующего импорта в другие программы.

В этом разделе:

- [Настройка соединения с прокси-сервером](#)

Чтобы открыть настройки сети

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Сеть**.

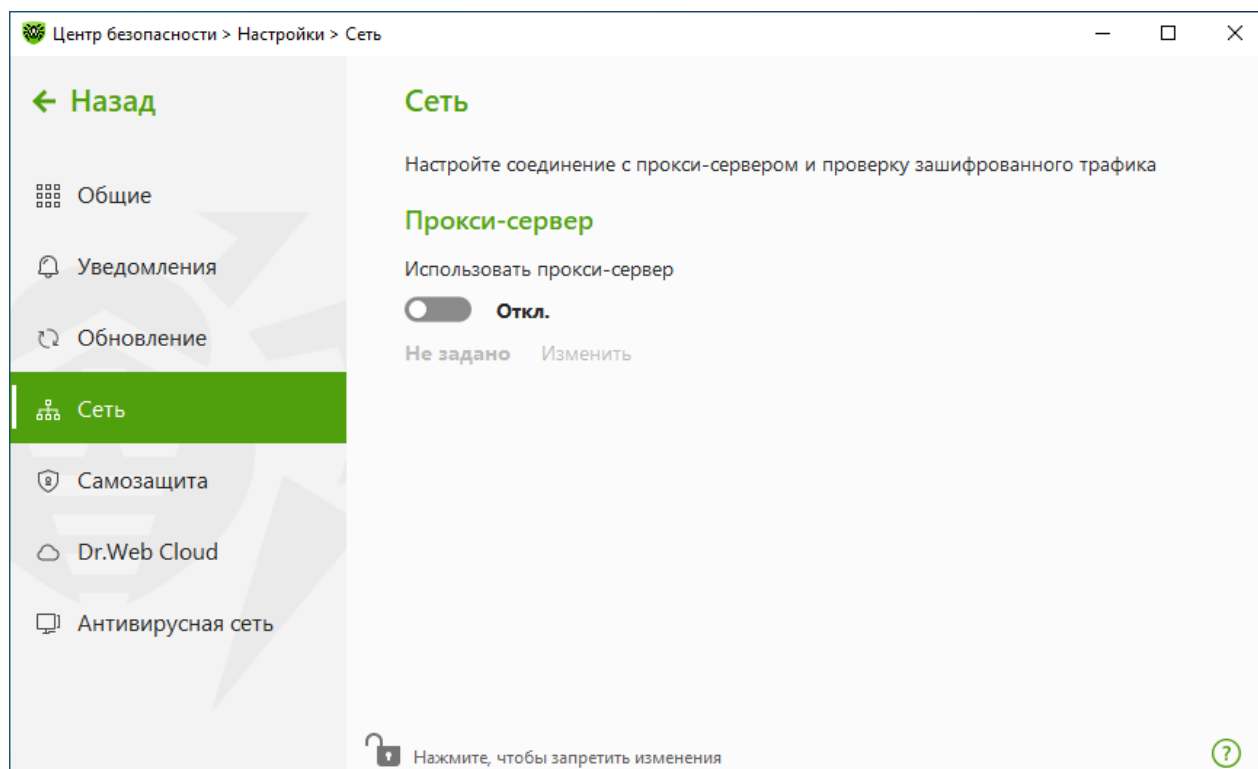


Рисунок 33. Подключение к прокси-серверу

Использование прокси-сервера

Вы можете включить режим использования прокси-сервера и задать настройки подключения к нему. Для этого:

1. Включите опцию **Использовать прокси-сервер** при помощи переключателя .
2. Нажмите ссылку **Изменить**, чтобы задать настройки подключения к прокси-серверу:

Настройка	Описание
Тип	Выберите протокол для подключения к прокси-серверу.
Адрес	Укажите адрес прокси-сервера.
Порт	Укажите порт прокси-сервера.
Логин	Укажите имя учетной записи для подключения к прокси-серверу.
Пароль	Укажите пароль учетной записи, используемой для подключения к прокси-серверу.
Тип авторизации	Выберите тип авторизации, требуемый для подключения к прокси-серверу (только для HTTP).



10.5. Самозащита

Вы можете настроить параметры защиты самого Dr.Web от несанкционированного воздействия, например от программ, вредоносное действие которых направлено на антивирусные программы, а также от случайного повреждения.

В этом разделе:

- [Включение и отключение самозащиты](#)
- [Запрет изменения даты и времени системы](#)

Чтобы перейти к настройкам Самозащиты

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Самозащита**.

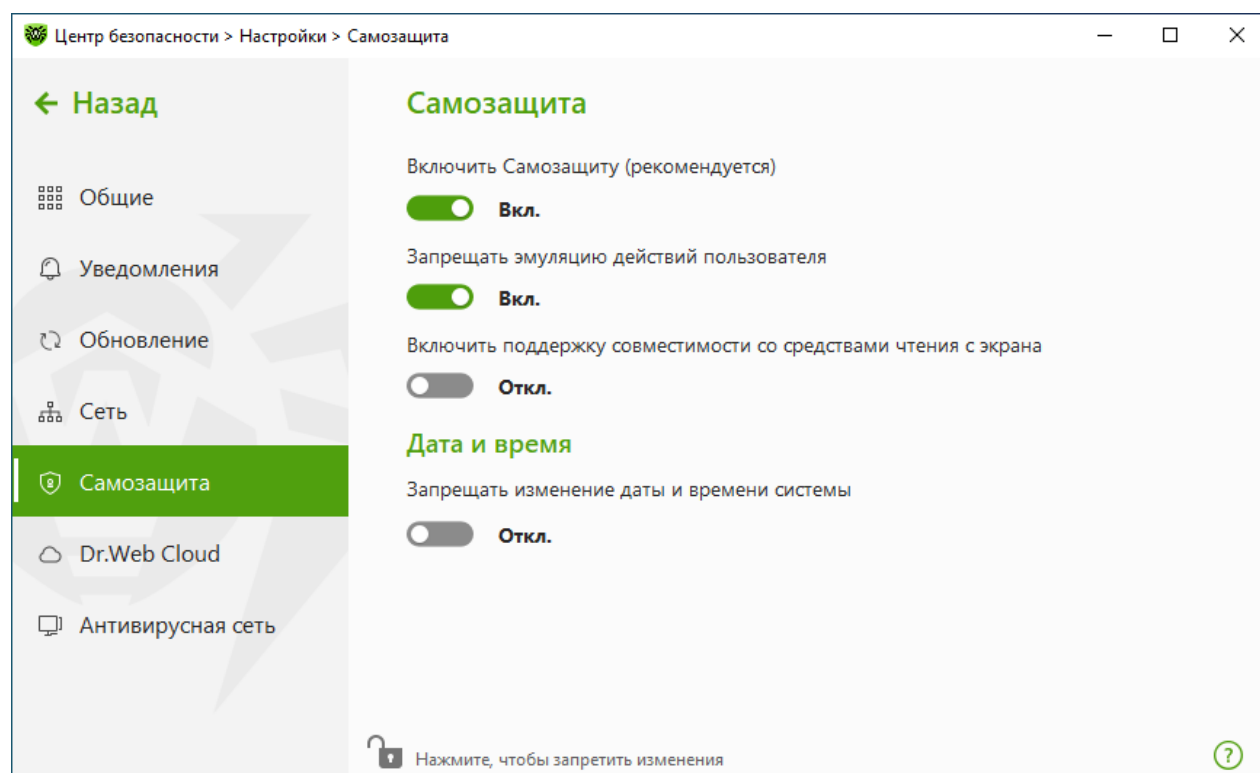


Рисунок 34. Параметры защиты Dr.Web



Настройки Самозащиты

Настройка **Включить Самозащиту (рекомендуется)** позволяет защитить файлы и процессы Dr.Web от несанкционированного доступа. Самозащита включена по умолчанию. Отключать Самозащиту не рекомендуется.



В случае возникновения проблем при использовании программ дефрагментации рекомендуется временно отключить модуль Самозащиты.

Чтобы произвести возврат к точке восстановления системы, необходимо отключить модуль Самозащиты.

Настройка **Запрещать эмуляцию действий пользователя** позволяет предотвратить изменения в настройках Dr.Web, производимые сторонними программными средствами. В том числе будет запрещено исполнение скриптов, эмулирующих работу клавиатуры и мыши в окнах Dr.Web (например, скриптов для изменения настроек Dr.Web, удаления лицензии и других действий, направленных на изменение работы Dr.Web).

Настройка **Включить поддержку совместимости со средствами чтения с экрана** позволяет использовать программы экранного доступа, такие как JAWS и NVDA, для озвучивания элементов интерфейса Dr.Web. Эта функция делает интерфейс программы доступным для людей с ограниченными возможностями.

Дата и время

Некоторые вредоносные программы намеренно изменяют системные дату и время. В этом случае лицензия может определяться как просроченная, и компоненты защиты будут отключены.

Настройка **Запрещать изменение даты и времени системы** позволяет заблокировать ручное и автоматическое изменение системных даты и времени, а также часового пояса. Это ограничение устанавливается для всех пользователей системы. Вы можете настроить [получение уведомлений](#) в том случае, если осуществлялась попытка изменить системное время.

10.6. Dr.Web Cloud

Вы можете подключиться к облачному сервису компании «Доктор Веб» и программе улучшения качества работы продуктов Dr.Web. Облачный сервис собирает информацию о последних угрозах на станциях пользователей, благодаря чему эффективно устраняются новейшие угрозы. Кроме того, обработка данных на облачном сервисе происходит быстрее, чем локально на компьютере пользователя.



В этом разделе:

- [Облачный сервис](#)
- [Программа улучшения качества ПО](#)

Чтобы включить или отключить Dr.Web Cloud

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Dr.Web Cloud**.
5. Включите или отключите Dr.Web Cloud при помощи переключателя .



Рисунок 35. Подключение к Dr.Web Cloud

Облачный сервис

Dr.Web Cloud позволяет антивирусной защите использовать свежую информацию об угрозах, обновляемую на серверах компании «Доктор Веб» в режиме реального времени.



Программа улучшения качества ПО

При участии в программе на сервера компании «Доктор Веб» будут автоматически отправляться обезличенные сведения о работе Dr.Web на вашем компьютере. Полученная информация не будет использоваться для идентификации пользователя или связи с ним.

Нажмите на ссылку **Политика конфиденциальности «Доктор Веб»**, чтобы ознакомиться с политикой конфиденциальности на [официальном сайте компании «Доктор Веб»](#) .

10.7. Удаленный доступ к Dr.Web

Вы можете разрешить удаленное управление вашим антивирусом с других компьютеров локальной сети при помощи компонента [Антивирусная сеть](#). Вхождение в состав антивирусной сети позволяет удаленно контролировать состояние антивирусной защиты (просматривать статистику, включать и отключать компоненты Dr.Web, изменять их настройки), а также получать обновления через локальную сеть. Чтобы использовать компьютер как источник обновлений для других компьютеров антивирусной сети, на которых установлен продукт Dr.Web, на нем нужно настроить [Зеркало обновлений](#).

Чтобы разрешить или запретить удаленное управление продуктом Dr.Web

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
3. В верхней части окна программы нажмите .
4. Откроется окно с основными настройками программы. В левой части окна выберите пункт **Антивирусная сеть**.
5. Разрешите или запретите удаленное управление продуктом Dr.Web при помощи переключателя .

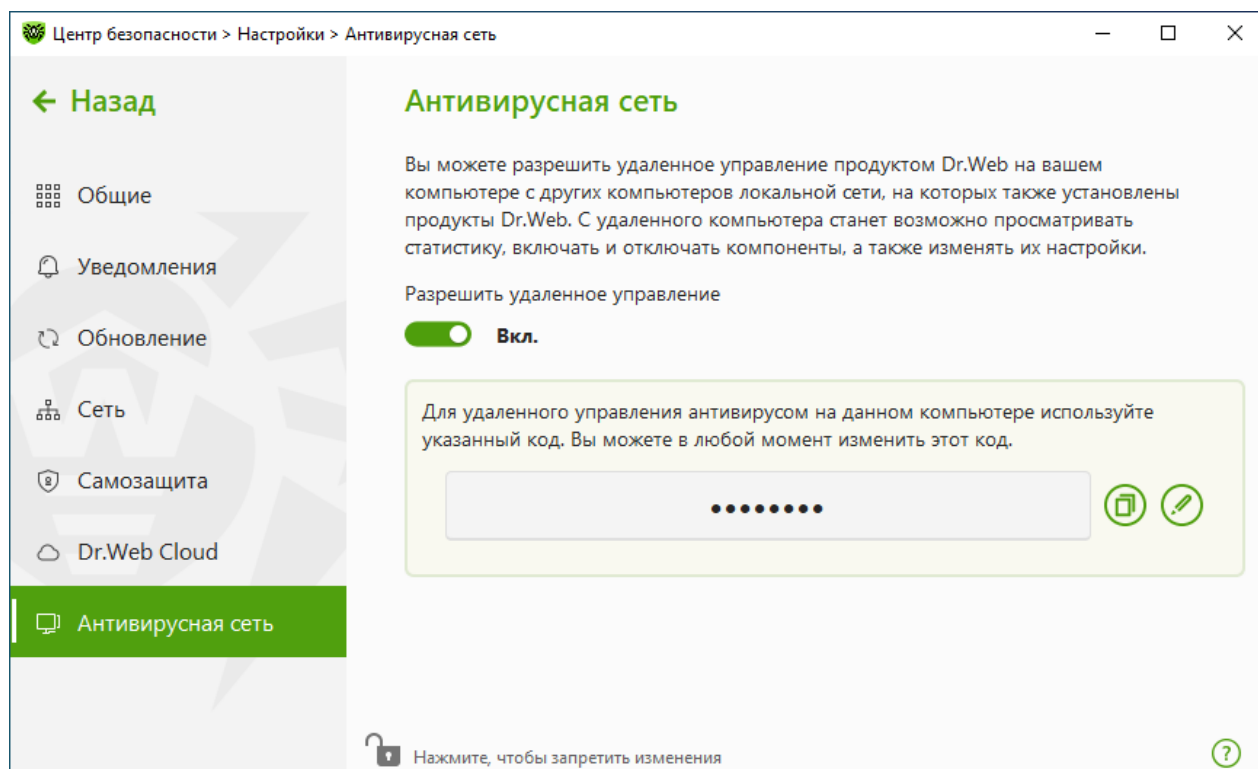


Рисунок 36. Включение удаленного управления антивирусом

Для удаленного управления Dr.Web на вашем компьютере необходимо будет вводить код. Вы можете использовать код, который автоматически генерируется при включении опции, или задать свой.

Удаленное управление позволяет просматривать статистику, включать и отключать модули, а также изменять их настройки. Компоненты Карантин, Защита от потери данных и Антивирусная сеть недоступны.



11. Превентивная защита

В данной группе настроек вы можете настроить реакцию Dr.Web на действия сторонних приложений, которые могут привести к заражению вашего компьютера, и выбрать уровень защиты от эксплойтов.

Чтобы перейти в группу настроек Превентивная защита

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Превентивная защита**.

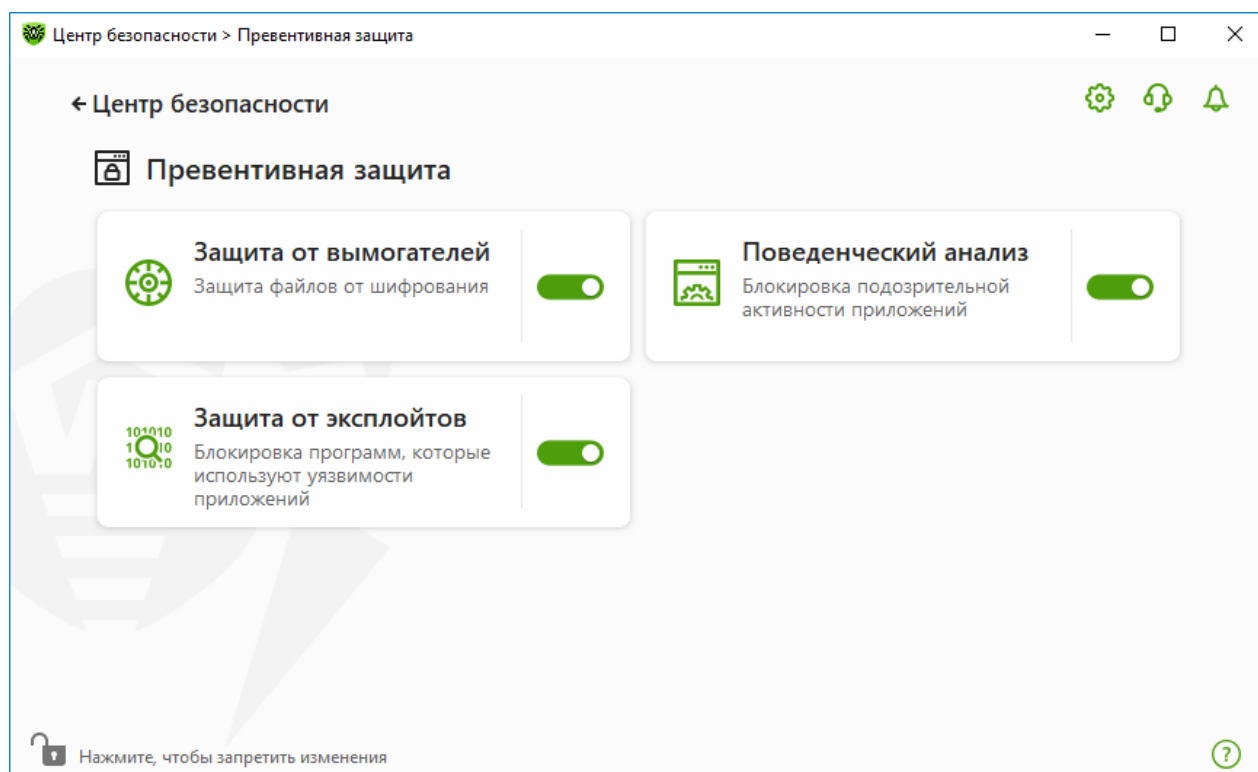


Рисунок 37. Окно Превентивная защита

Включение и отключение компонентов защиты

Включите или отключите необходимый компонент при помощи переключателя .

Чтобы перейти к параметрам компонентов

1. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
2. Нажмите плитку необходимого компонента.

В этом разделе:

- [Защита от вымогателей](#) — параметры запрета шифрования файлов пользователей.



- **Поведенческий анализ** — параметры запрета доступа приложений к системным объектам.
- **Защита от эксплойтов** — параметры запрета использования уязвимостей в приложениях.



Чтобы *отключить* какой-либо из компонентов, Dr.Web должен работать в режиме администратора. Для этого нажмите на замок  в нижней части окна программы.

11.1. Защита от вымогателей

Компонент Защита от вымогателей позволяет отслеживать процессы, которые пытаются зашифровать пользовательские файлы по известному алгоритму, свидетельствующему о том, что такие процессы являются угрозой безопасности компьютера. К таким процессам относятся *троянцы-шифровальщики*. Данные вредоносные программы, попадая на компьютер пользователя, блокируют доступ к данным, после чего вымогают деньги за расшифровку. Они являются одними из самых распространенных вредоносных программ и ежегодно приносят большие убытки как компаниям, так и обычным пользователям. Основной путь заражения — почтовые рассылки, содержащие вредоносный файл или ссылку на вредоносную программу.

По статистике компании «Доктор Веб» расшифровка поврежденных троянцем файлов возможна только в 10 % случаев, поэтому наиболее эффективный метод борьбы — предотвратить заражение. В последнее время число пользователей, пострадавших от данного типа угроз, снижается. Тем не менее, количество запросов в службу технической поддержки компании «Доктор Веб» на расшифровку данных достигает 1000 в месяц.

Чтобы включить или отключить компонент Защита от вымогателей

1. Откройте **меню** Dr.Web  и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Превентивная защита**.
3. Включите или отключите компонент Защита от вымогателей при помощи переключателя .

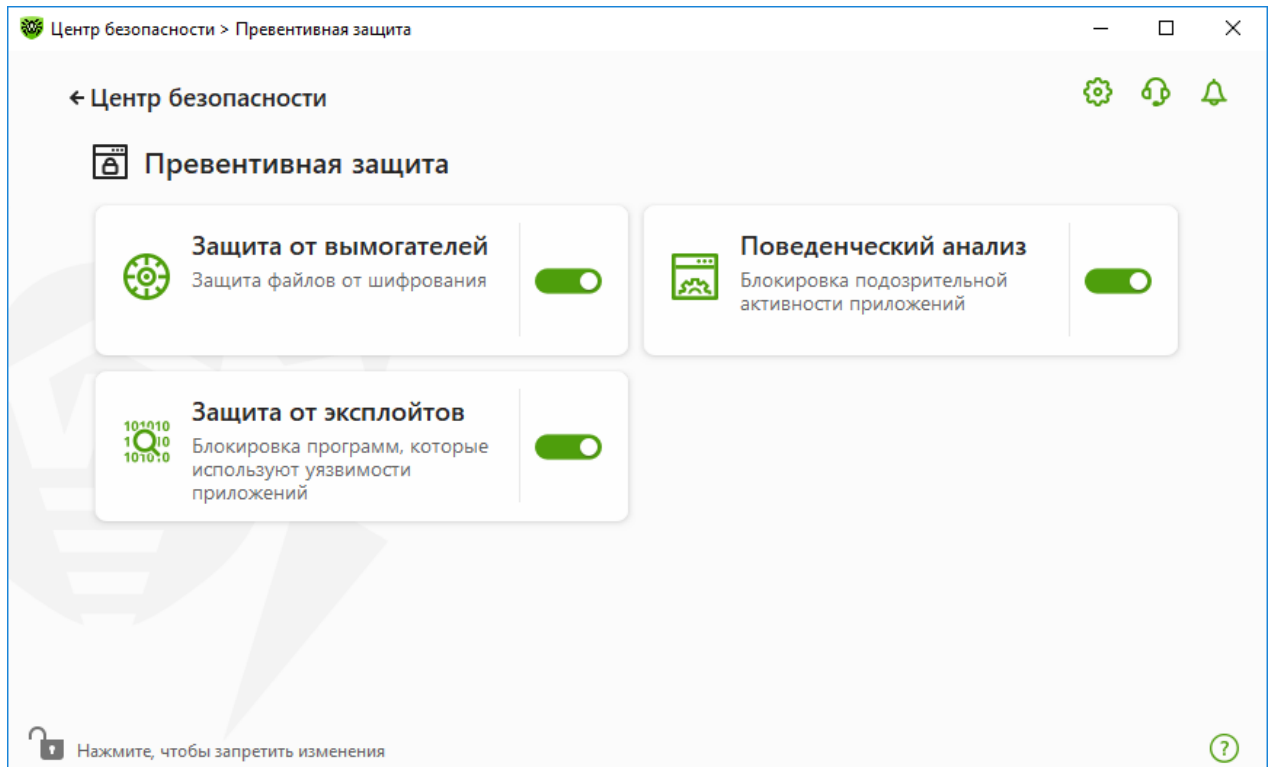


Рисунок 38. Включение/отключение компонента Защита от вымогателей

В этом разделе:

- [Настройка реакции на попытки приложений зашифровать файлы](#)
- [Исключения из проверки](#)

Реакция Dr.Web на попытки приложений зашифровать файл

Чтобы настроить параметры компонента Защита от вымогателей

1. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. Нажмите плитку **Защита от вымогателей**. Откроется окно параметров компонента.
3. В выпадающем меню выберите действие, которое будет применяться для всех приложений.

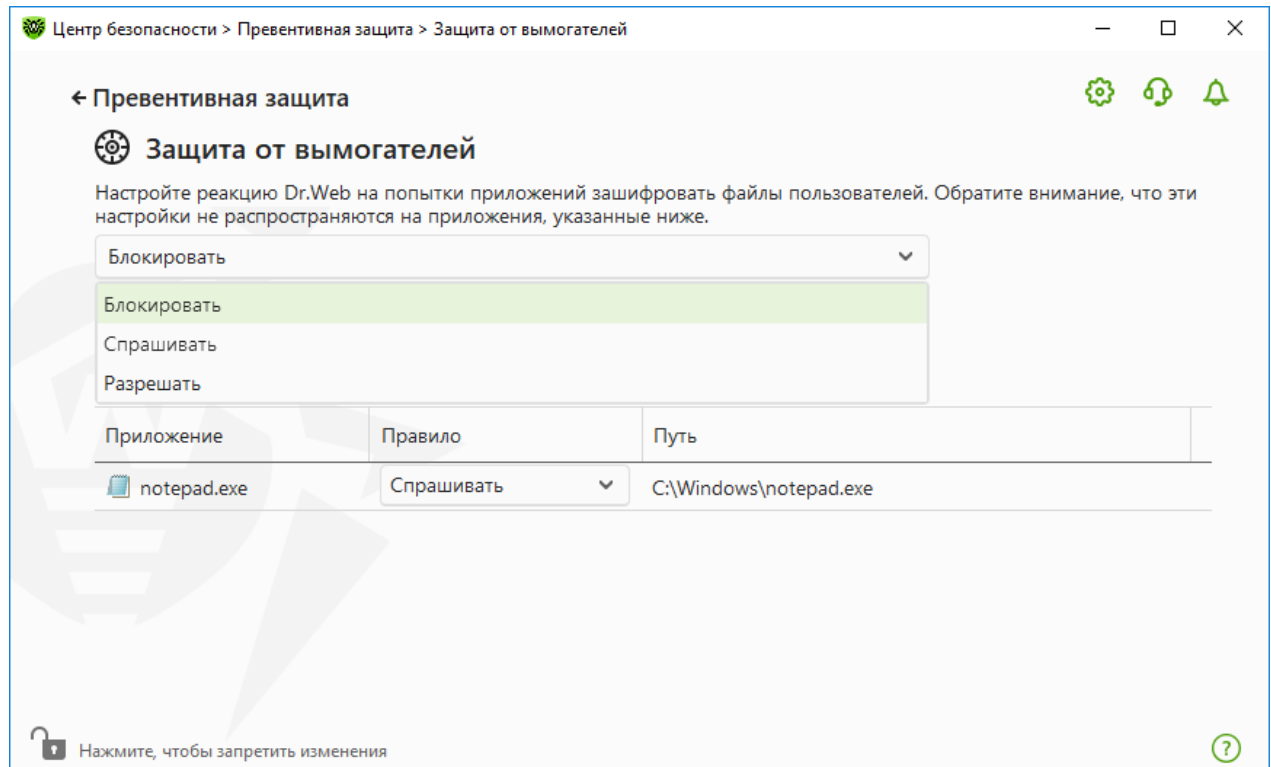


Рисунок 39. Выбор реакции Dr.Web

- **Разрешать** — всем приложениям будет разрешено модифицировать файлы пользователя.
- **Блокировать** — всем приложениям будет запрещено шифровать файлы пользователя. Этот режим установлен по умолчанию. При попытке приложения зашифровать файлы пользователя будет показано уведомление:

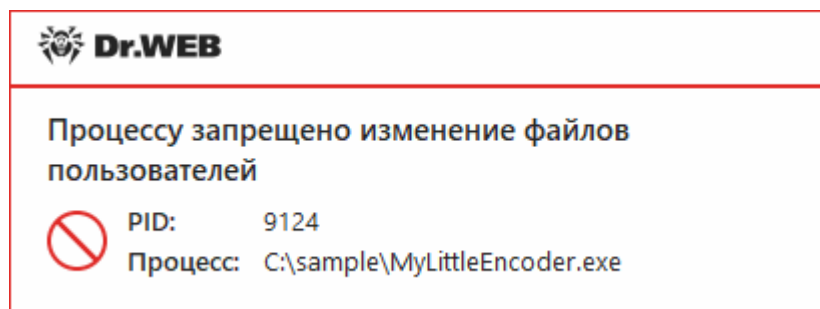


Рисунок 40. Пример уведомления о запрете изменения файлов пользователя

- **Спрашивать** — при попытке приложения зашифровать файл пользователя будет показываться уведомление, где вы сможете запретить приложению это действие или проигнорировать его:

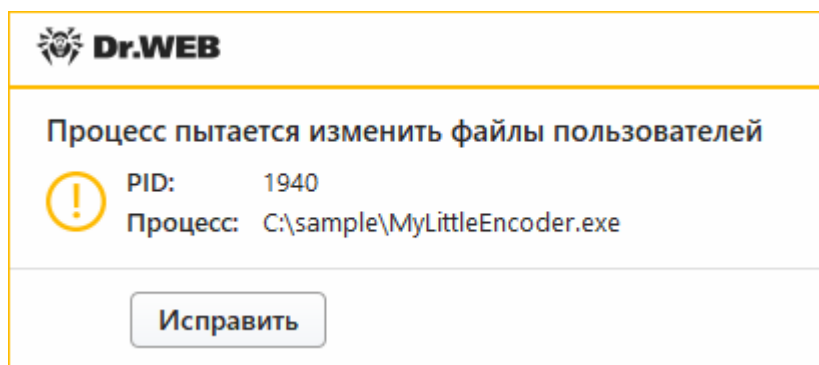


Рисунок 41. Пример уведомления о попытке изменения файлов пользователя

- Если вы нажмете кнопку **Исправить**, процесс будет заблокирован и занесен в карантин. Даже при восстановлении приложения из карантина оно не сможет быть запущено до перезагрузки компьютера.
- Если вы закроете окно уведомления, приложение не будет обезврежено.

Получение уведомлений

Вы можете [настроить](#) вывод уведомлений о действиях компонента Защита от вымогателей на экран и отправку этих уведомлений на электронную почту.

См. также:

- [Уведомления](#)

Список приложений, исключенных из проверки

Вы можете сформировать список приложений, которые будут исключены из проверок компонентом Защита от вымогателей. Для работы с объектами в списке доступны следующие элементы управления:

- Кнопка  — добавление приложения в исключение из проверки.
- Кнопка  — удаление приложения из списка исключений.

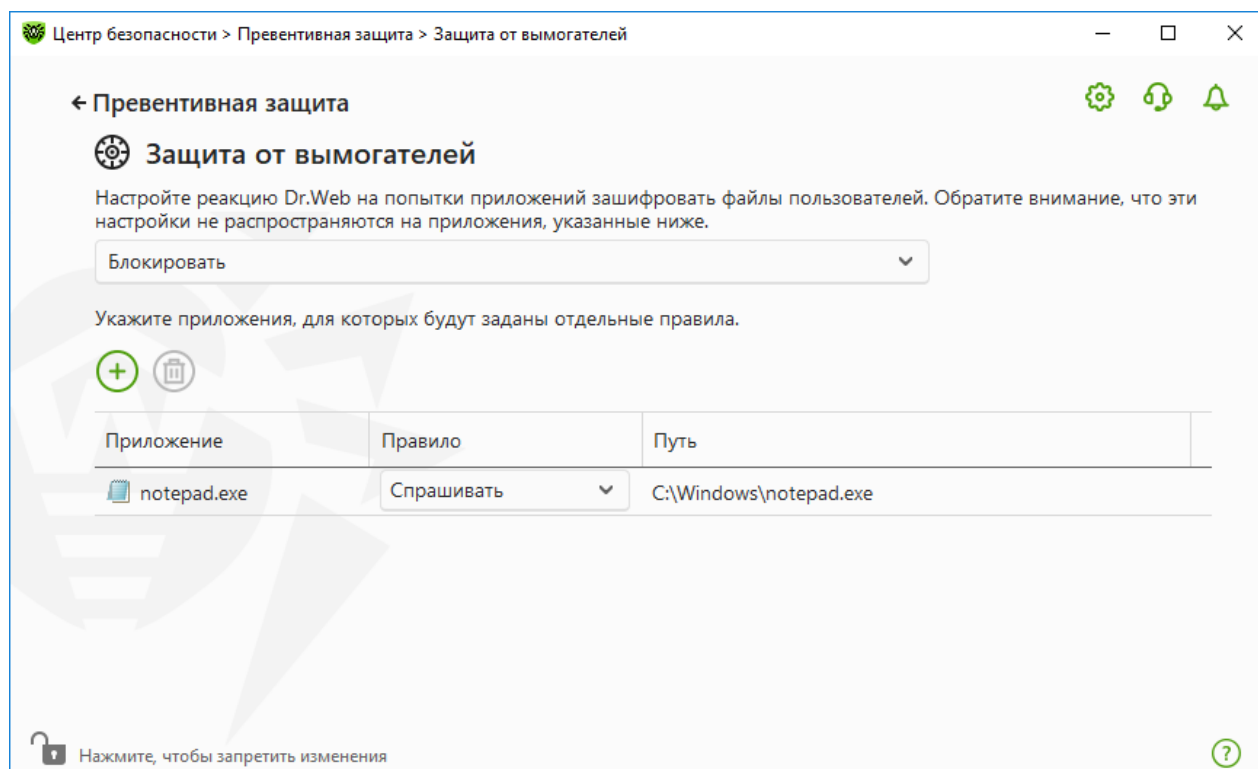


Рисунок 42. Исключения из проверки Защитой от вымогателей

Чтобы добавить приложение в список

1. Нажмите кнопку  и в открывшемся окне выберите необходимое приложение.
2. Нажмите **ОК**.

Чтобы защитить свои данные от несанкционированных изменений, вы можете также [добавить файлы в список защищенных](#).

11.2. Поведенческий анализ

Компонент Поведенческий анализ позволяет настроить реакцию Dr.Web на действия сторонних приложений, не являющихся доверенными, которые могут привести к заражению вашего компьютера, например на попытки модифицировать файл HOSTS или изменить критически важные системные ветки реестра. При включении компонента Поведенческий анализ программа запрещает автоматическое изменение системных объектов, модификация которых однозначно свидетельствует о попытке вредоносного воздействия на операционную систему. Поведенческий анализ защищает систему от ранее неизвестных вредоносных программ, которые способны избежать обнаружения традиционными сигнатурными и эвристическими механизмами. Для определения вредоносности приложений используются наиболее актуальные данные облачного сервиса Dr.Web.



Чтобы включить или отключить компонент Поведенческий анализ

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Превентивная защита**.
3. Включите или отключите компонент Поведенческий анализ при помощи переключателя .

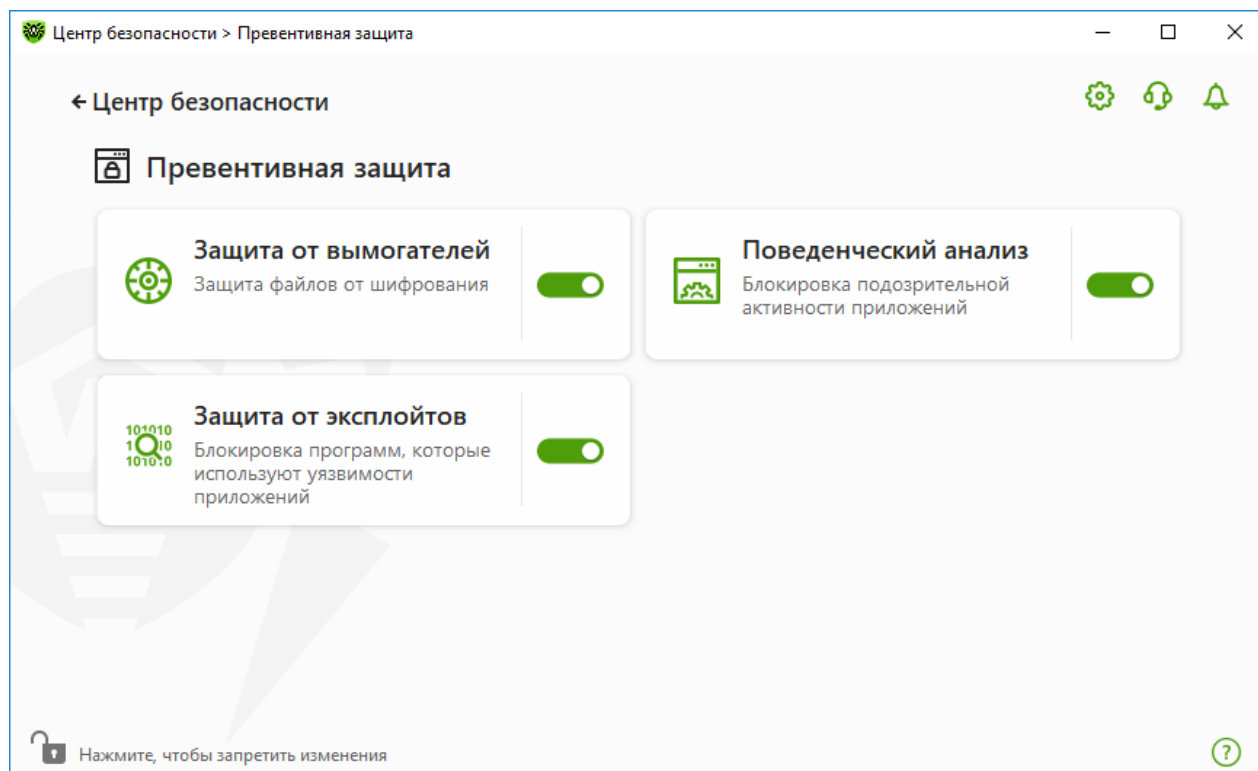


Рисунок 43. Включение/отключение компонента Поведенческий анализ

В этом разделе:

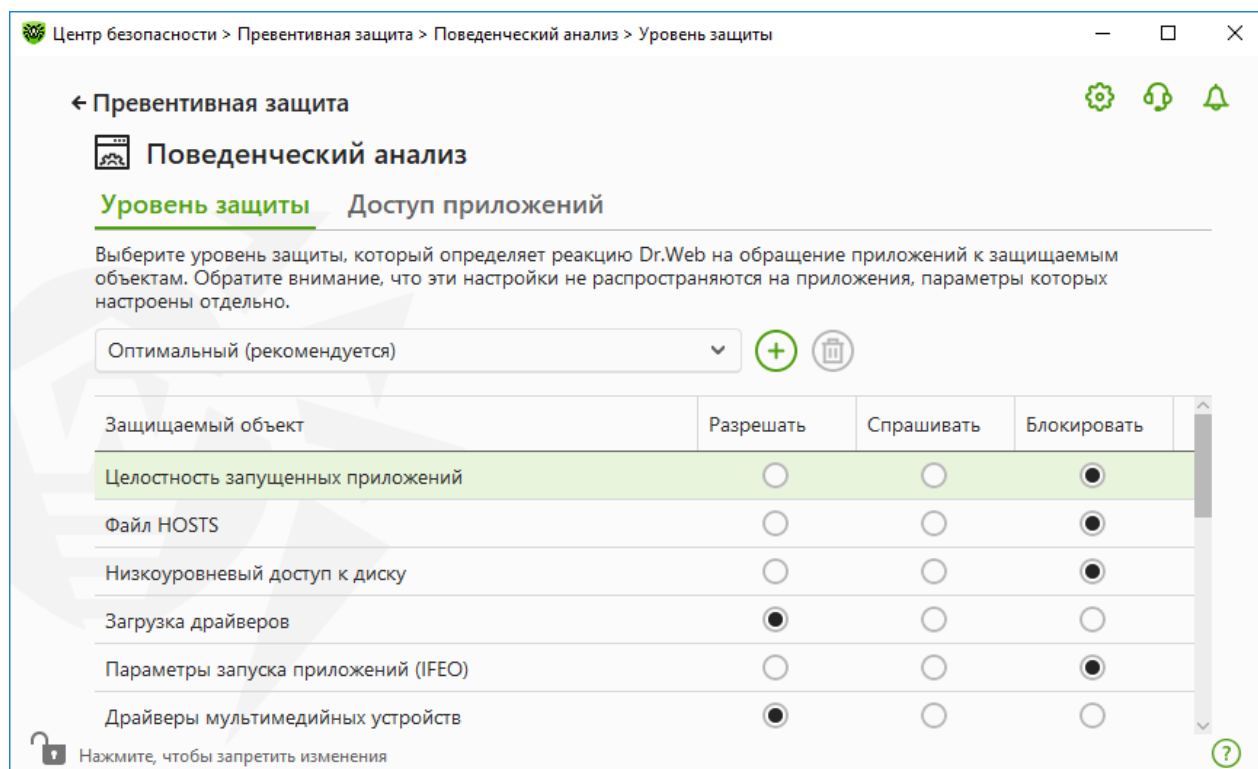
- [Режимы работы компонента](#)
- [Создание и изменение отдельных правил для приложений](#)
- [Описание защищаемых объектов](#)

Параметры Поведенческого анализа

Настройки программы по умолчанию являются оптимальными в большинстве случаев, их не следует изменять без необходимости.

Чтобы перейти к параметрам компонента Поведенческий анализ

1. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
2. Нажмите плитку **Поведенческий анализ**. Откроется окно параметров компонента.

**Рисунок 44. Параметры Поведенческого анализа**

Вы можете задать отдельный уровень защиты для конкретных объектов и процессов и общий уровень, настройки которого будут применяться ко всем остальным процессам. Для задания общего уровня защиты на вкладке **Уровень защиты** выберите необходимый уровень из выпадающего списка.

Уровни защиты

Уровень защиты	Описание
Оптимальный (рекомендуется)	Используется по умолчанию. Dr.Web запрещает автоматическое изменение системных объектов, модификация которых однозначно свидетельствуют о попытке вредоносного воздействия на операционную систему. Также запрещаются низкоуровневый доступ к диску и модификация файла HOSTS приложениям, действия которых однозначно определяются как попытка вредоносного воздействия на операционную систему.  Блокируются только действия приложений, которые не являются доверенными.
Средний	Этот уровень защиты можно установить при повышенной опасности заражения. В данном режиме дополнительно запрещается доступ к тем критическим объектам, которые могут потенциально использоваться вредоносными программами.



Уровень защиты	Описание
	 В данном режиме защиты возможны конфликты совместимости со сторонним программным обеспечением, использующим защищаемые ветки реестра.
Параноидальный	Этот уровень защиты необходим для полного контроля за доступом к критическим объектам Windows. В данном режиме вам также будет доступен интерактивный контроль за загрузкой драйверов и автоматическим запуском программ.
Пользовательский	В этом режиме вы можете выбрать уровни защиты для каждого объекта по своему усмотрению.

Пользовательский режим

Все изменения в настройках сохраняются в Пользовательском режиме работы. В этом окне вы также можете создать новый уровень защиты для сохранения нужных настроек. При любых настройках компонента защищаемые объекты будут доступны для чтения.

Вы можете выбрать одну из реакций Dr.Web на попытки приложений модифицировать защищаемые объекты:

- **Разрешать** — доступ к защищаемому объекту будет разрешен для всех приложений.
- **Спрашивать** — при попытке приложения модифицировать защищаемый объект будет показано уведомление:

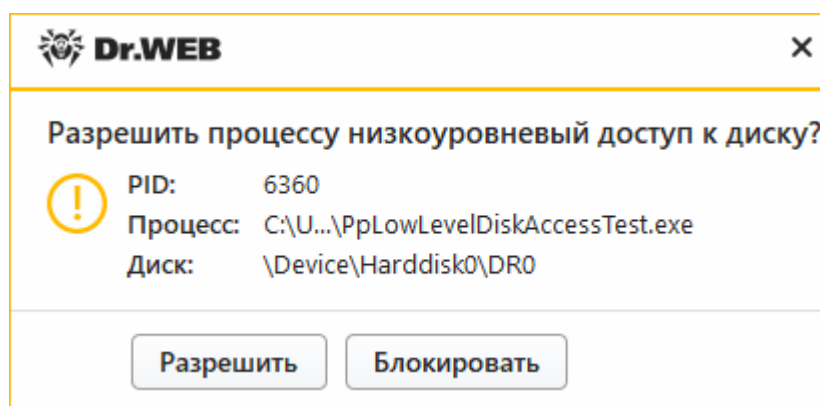


Рисунок 45. Пример уведомления с запросом доступа к защищаемому объекту

- **Блокировать** — при попытке приложения модифицировать защищаемый объект приложению будет отказано в доступе. При этом будет показано уведомление:

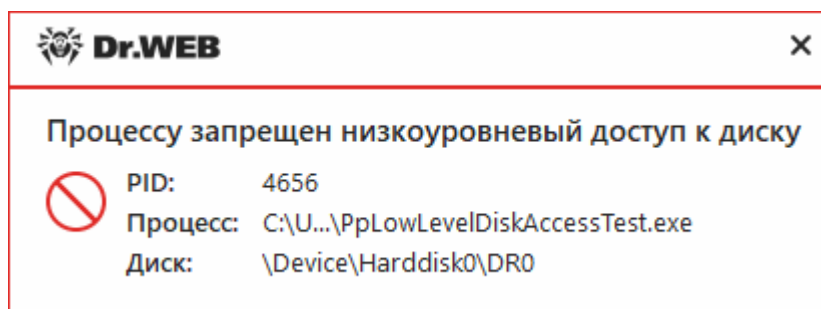


Рисунок 46. Пример уведомления о запрете доступа к защищаемому объекту

Чтобы создать новый уровень защиты

1. Просмотрите настройки защиты, заданные по умолчанию и, при необходимости, отредактируйте их.
2. Нажмите кнопку .
3. В открывшемся окне укажите название для нового профиля.
4. Нажмите **ОК**.

Чтобы удалить уровень защиты

1. Из выпадающего списка выберите созданный уровень защиты, который вы хотите удалить.
2. Нажмите кнопку . Предусмотренные профили удалить нельзя.
3. Нажмите **ОК**, чтобы подтвердить удаление.

Получение уведомлений

Вы можете [настроить](#) вывод уведомлений о действиях компонента Поведенческий анализ на экран и отправку этих уведомлений на электронную почту.

См. также:

- [Уведомления](#)

Доступ приложений

Чтобы задать отдельные параметры доступа для конкретных приложений, перейдите на вкладку **Доступ приложений**. Здесь вы можете добавить новое правило для приложения, отредактировать уже созданное правило или удалить ненужное.

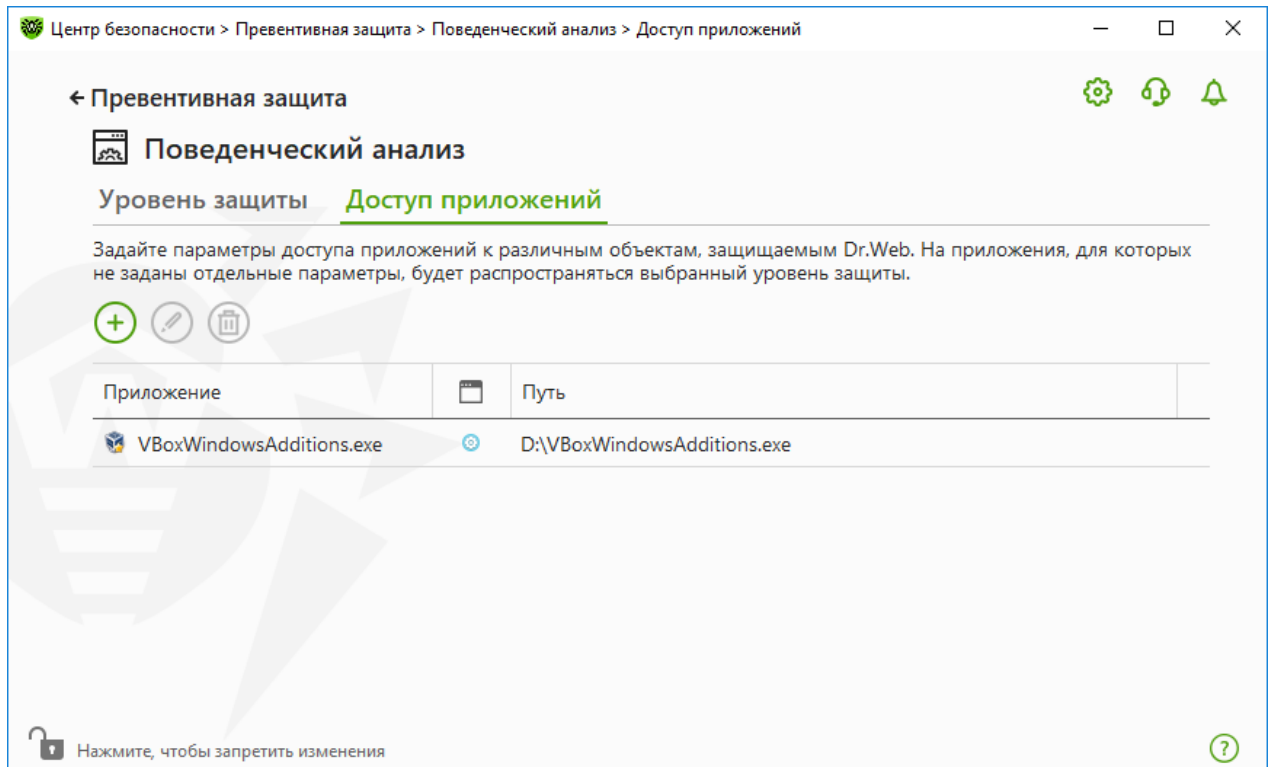


Рисунок 47. Параметры доступа для приложений

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка — добавление набора правил для приложения.
- Кнопка — редактирование существующих наборов правил.
- Кнопка — удаление набора правил.

В столбце (**Тип правила**) может отображаться три типа правил:

- — задано правило **Разрешать все** для всех защищаемых объектов.
- — заданы разные правила для защищаемых объектов.
- — задано правило **Блокировать все** для всех защищаемых объектов.

Чтобы добавить правило для приложения

1. Нажмите кнопку .
2. В открывшемся окне нажмите кнопку **Обзор** и укажите путь к исполняемому файлу приложения.

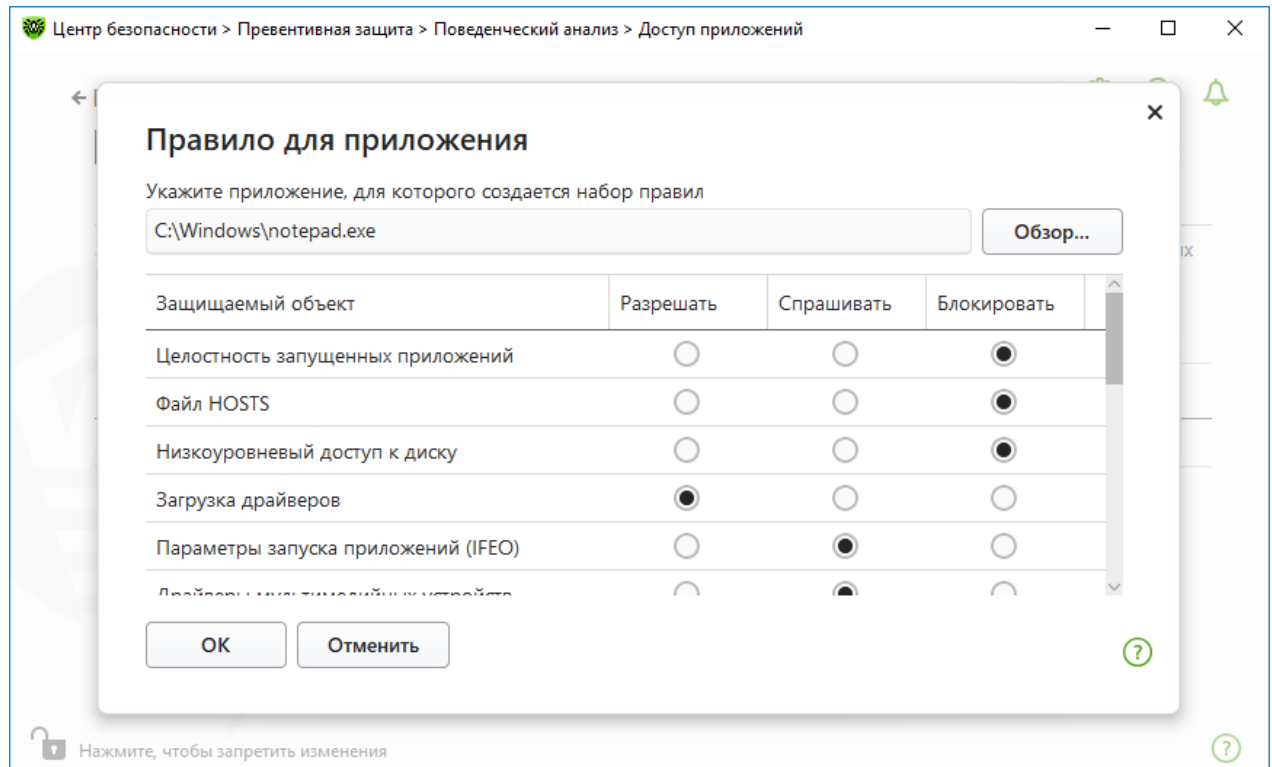


Рисунок 48. Добавление набора правил для приложения

3. Просмотрите настройки защиты, заданные по умолчанию и, при необходимости, отредактируйте их.
4. Нажмите **ОК**.

Защищаемые объекты

Защищаемый объект	Описание
Целостность запущенных приложений	Данная настройка позволяет отслеживать процессы, которые внедряются в запущенные приложения, что является угрозой безопасности компьютера.
Файл HOSTS	Файл HOSTS используется операционной системой для упрощения доступа к интернету. Изменения этого файла могут быть результатом работы вируса или другой вредоносной программы.
Низкоуровневый доступ к диску	Данная настройка позволяет запрещать приложениям запись на жесткий диск посекторно, не обращаясь к файловой системе.
Загрузка драйверов	Данная настройка позволяет запрещать приложениям загрузку новых или неизвестных драйверов.

Прочие настройки позволяют защищать от модификации ветки реестра (как в системном профиле, так и в профилях всех пользователей).



Защищаемый объект	Описание
Параметры запуска приложений (IFEO)	• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Драйверы мультимедийных устройств	• Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers
Параметры оболочки Winlogon	• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL
Нотификаторы Winlogon	• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
Автозапуск оболочки Windows	• Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib
Ассоциации исполняемых файлов	• Software\Classes\ .exe, .pif, .com, .bat, .cmd, .scr, .lnk (ключи) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (ключи)
Политики ограничения запуска программ (SRP)	• Software\Microsoft\Windows\CurrentVersion\Group Policy Objects*\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers • Software\Microsoft\Windows\CurrentVersion\Group Policy Objects*\Software\Policies\Microsoft\Windows\SrpV2 • Software\Policies\Microsoft\Windows\Safer • Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers • Software\Policies\Microsoft\Windows\SrpV2
Плагины Internet Explorer (BHO)	• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
Автозапуск программ	• Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup • Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
Автозапуск политик	• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run



Защищаемый объект	Описание
Конфигурация безопасного режима	• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network
Параметры Менеджера сессий	• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows
Системные службы	• System\CurrentControlSetXXX\Services



Если при установке важных обновлений от Microsoft или при установке и работе программ (в том числе программ дефрагментации) возникают проблемы, временно отключите Поведенческий анализ.

11.3. Защита от эксплойтов

Компонент Защита от эксплойтов позволяет блокировать вредоносные объекты, которые используют уязвимости в популярных приложениях. При определении вредоносности объекта используются в том числе данные из облачного сервиса Dr.Web.

Чтобы включить или отключить компонент Защита от эксплойтов

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Превентивная защита**.
3. Включите или отключите компонент Защита от эксплойтов при помощи переключателя .

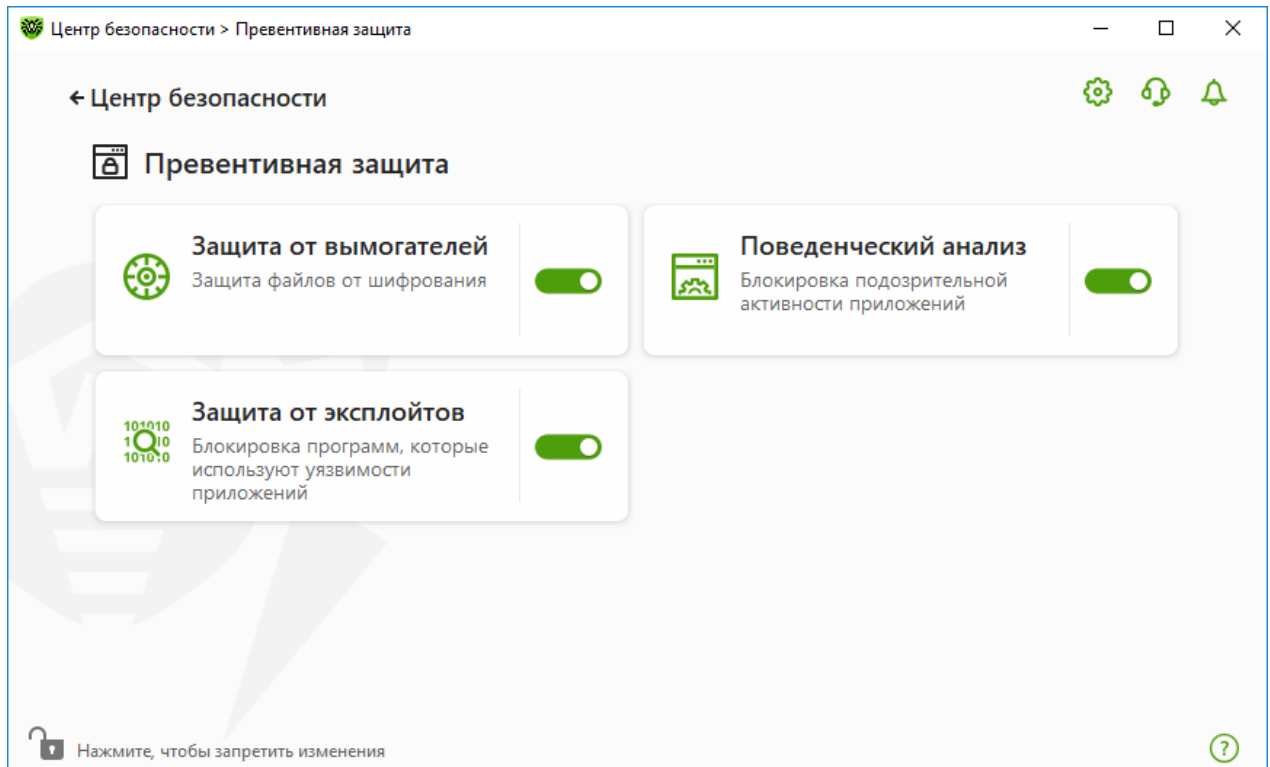


Рисунок 49. Включение/отключение компонента Защита от эксплойтов

Чтобы перейти к параметрам компонента Защита от эксплойтов

1. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт»). В противном случае нажмите на замок .
2. Нажмите плитку **Защита от эксплойтов**. Откроется окно параметров компонента.

В соответствующем выпадающем списке в окне параметров компонента выберите подходящий уровень защиты от эксплойтов.

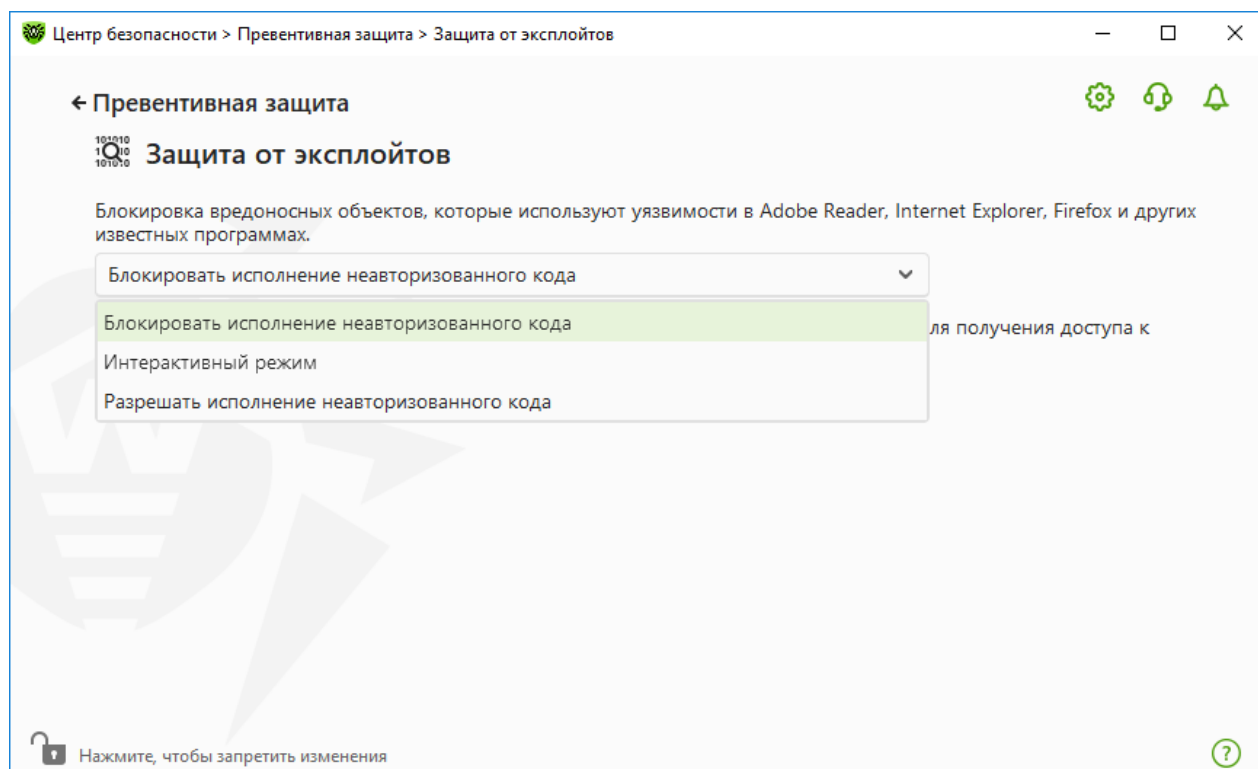


Рисунок 50. Выбор уровня защиты

Уровни защиты

Уровень защиты	Описание
Блокировать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически заблокирована.
Интерактивный режим	При попытке вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы Dr.Web выведет соответствующее сообщение. Ознакомьтесь с информацией и выберите нужное действие.
Разрешать исполнение неавторизованного кода	Попытка вредоносного объекта использовать уязвимости в программном обеспечении для получения доступа к критическим областям операционной системы будет автоматически разрешена.

Получение уведомлений

Вы можете [настроить](#) вывод уведомлений о действиях компонента Защита от эксплойтов на экран и отправку этих уведомлений на электронную почту.

См. также:

- [Уведомления](#)



12. Защита от потери данных

Защита от потери данных — функция, которая обеспечивает защиту содержимого важных папок от изменений вредоносным программным обеспечением. Вы можете свободно просматривать и добавлять файлы в защищенную папку, однако любая модификация файлов в ней или удаление запрещены. Чтобы разрешить приложениям доступ к папке, можно добавить необходимые приложения в исключения. Также вы можете восстановить ранее сохраненные копии.

Чтобы перейти в окно Защита от потери данных

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. Нажмите плитку **Защита от потери данных**.

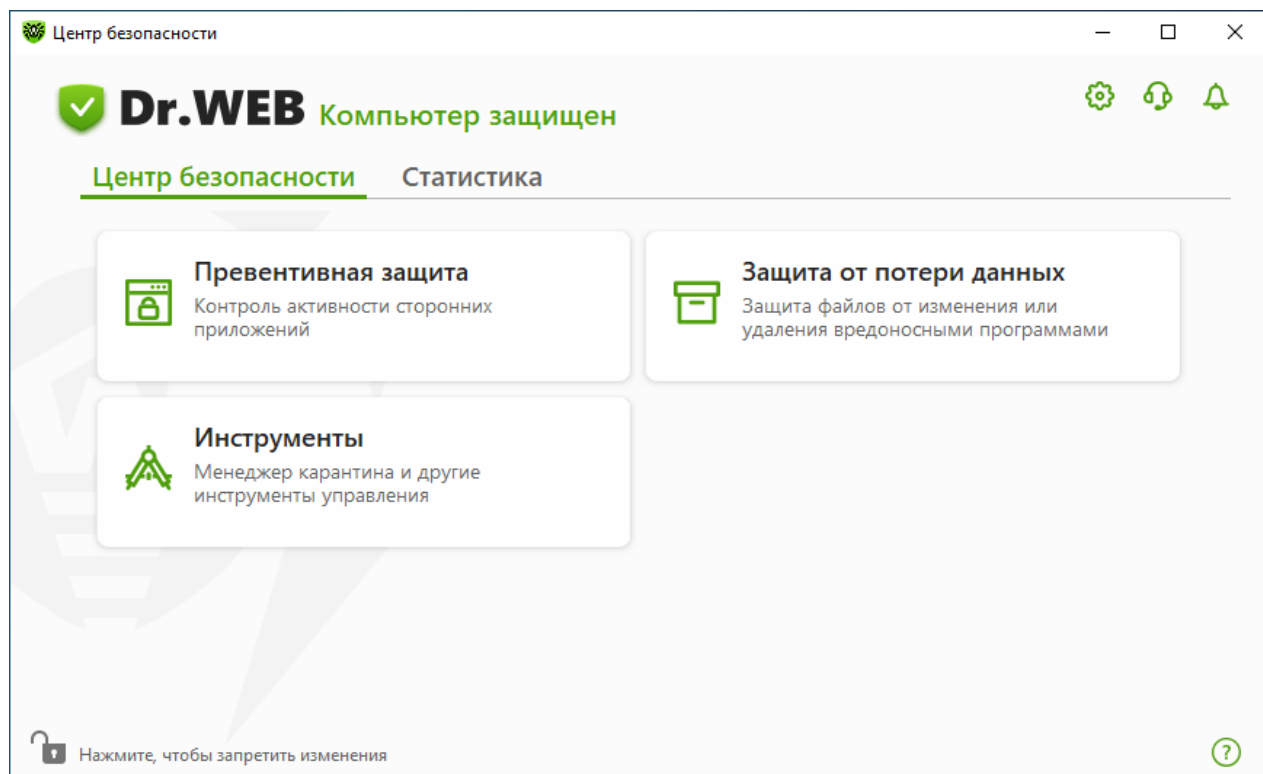


Рисунок 51. Доступ к окну Защита от потери данных

В этом разделе:

- [Особенности работы при наличии сохраненных копий файлов](#)
- [Управление защищаемыми папками](#)
- [Исключения](#)
- [Восстановление и удаление сохраненных копий](#)



Защищаемые папки

Для каждой папки вы можете настроить параметры доступа для приложений. Защищенная папка будет доступна для просмотра и копирования. Также будет доступно создание новых элементов в папке и их модификация процессами, создавшими новые элементы, до тех пор, пока эти процессы не завершены. При обращении приложений к папке будет показываться уведомление о запрете доступа.



В случае обнаружения угрозы доступ к удалению и модификации файлов в защищенных папках остается только у Dr.Web.

При добавлении папки в список защищенных действует правило по умолчанию — запрет на любые модификации и удаление содержимого папки всем приложениям, кроме приложений из списка доверенных. Со списком доверенных приложений можно ознакомиться на сайте https://products.drweb.com/services/data_protection/. Список включает наиболее популярные приложения, такие как некоторые приложения Microsoft и Adobe. Системные процессы, такие как `explorer.exe`, не входят в список доверенных, поскольку могут быть использованы вредоносными объектами для атак на систему.



Не допускается добавление системных папок в список защищаемых, поскольку это может привести к критическим ошибкам в работе системы.

Защита от потери данных распространяется только на локальные (расположенные физически на вашем устройстве) файлы и папки в рамках той же операционной системы, на которой настраивается защита. При наличии на одном компьютере нескольких операционных систем защиту от потери данных необходимо настраивать отдельно на каждой системе. Защита сетевых дисков и папок невозможна.

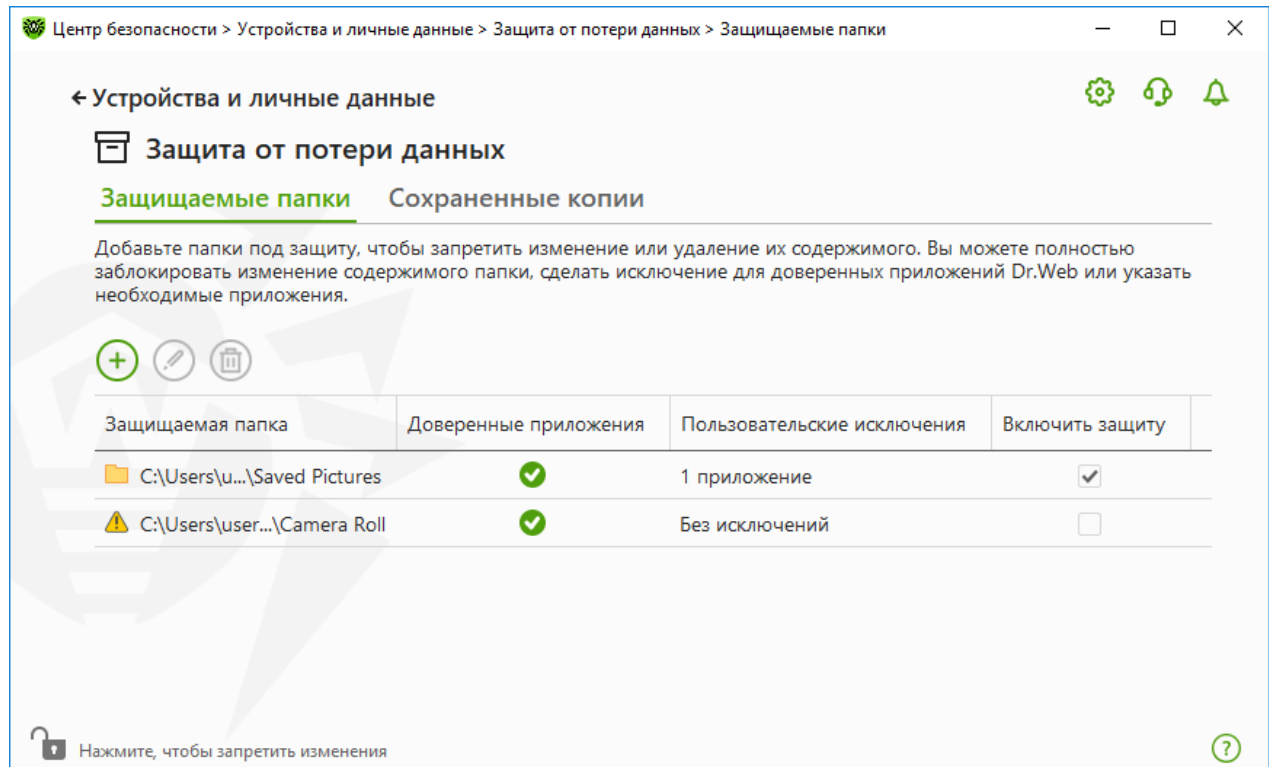


Рисунок 52. Защищаемые папки

В таблице выводится информация о:

- защищаемом объекте;
- количестве исключений из общего правила;
- статусе защиты.

Для активации функции защиты объекта установите флажок в столбце **Включить защиту** напротив необходимого объекта. При снятии флажка защита с папки полностью снимается и папка отображается со знаком ⚠.

Для работы с объектами в таблице доступны следующие элементы управления:

- Кнопка — добавление объекта в список защищенных;
- Кнопка — редактирование элементов в таблице;
- Кнопка — удаление объекта из списка защищенных.

Чтобы добавить папку в список защищаемых

1. Нажмите кнопку . В открывшемся окне выберите необходимый объект, нажав кнопку **Обзор**.
2. При необходимости включите или выключите доступ к папке доверенным приложениям. По умолчанию опция включена.
3. Вы также можете указать приложения, которые будут иметь полный доступ к объекту вне зависимости от общих настроек.

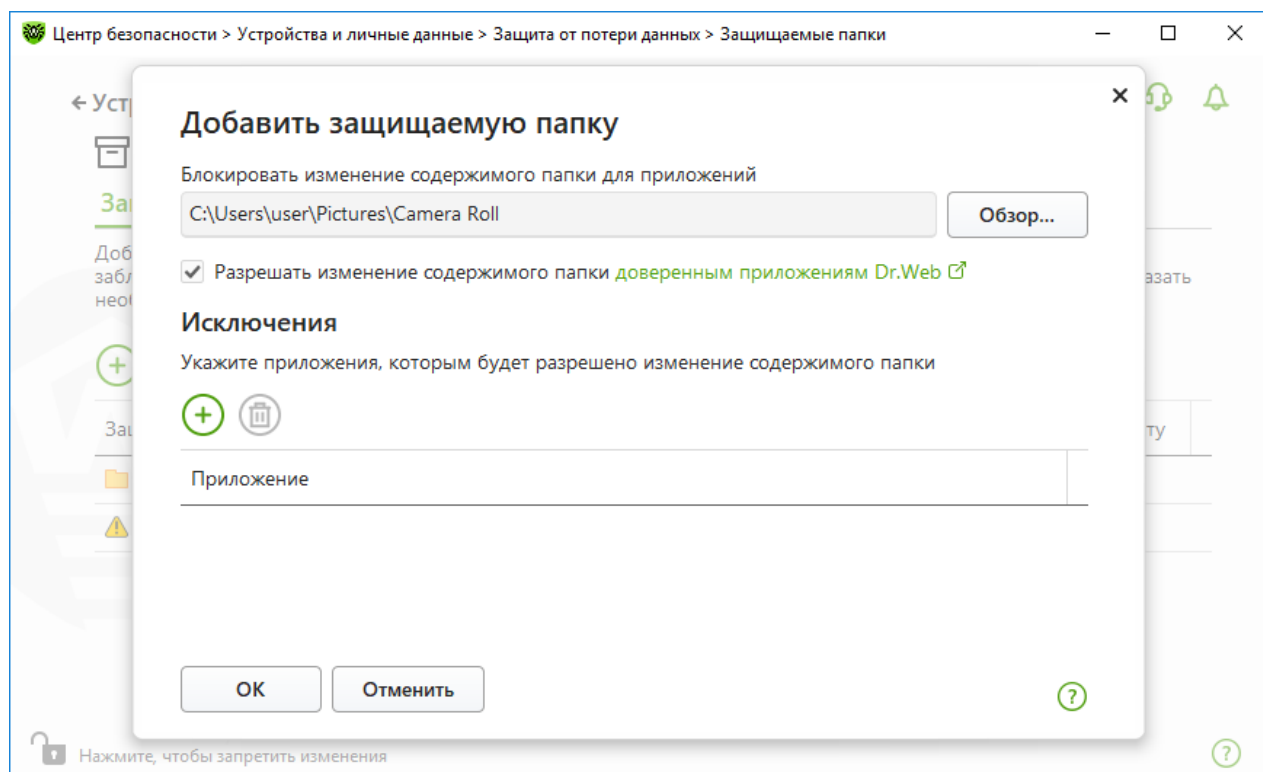


Рисунок 53. Добавление защищаемой папки

Исключения

Количество приложений, имеющих полный доступ к защищаемой папке, указано на главном окне Защиты от потери данных в столбце **Пользовательские исключения**.

Чтобы добавить приложение в исключения

1. В окне [Защита от потери данных](#) нажмите , чтобы добавить новую папку в список защищаемых.
2. В открывшемся окне нажмите . Выберите приложение, которое будет иметь полный доступ к объектам в защищаемой папке.
3. Нажмите **ОК**.

Чтобы изменить список исключений для защищаемых папок

1. Выберите папку из списка и нажмите .
2. В нижней части открывшегося окна в таблице указаны все приложения, которые имеют полный доступ к выбранной папке.
 - Чтобы добавить новое приложение, нажмите .
 - Чтобы удалить приложение из списка исключений, нажмите .
3. Нажмите **ОК**.



Сохраненные копии

Вкладка доступна, только если остались сохраненные в предыдущих версиях программы копии файлов. Функция позволяет восстановить или удалить сохраненные копии, но сохранение новых копий недоступно.

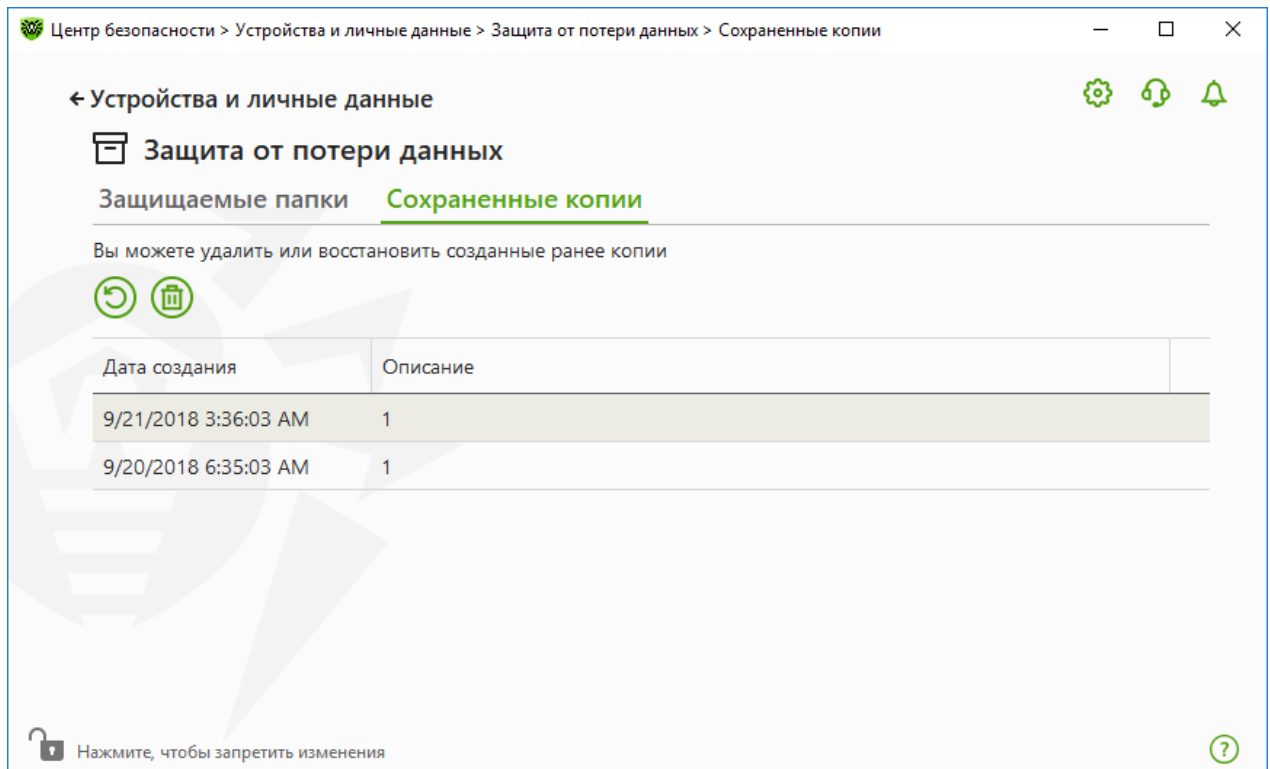


Рисунок 54. Список сохраненных копий

Удаление созданных копий

Вы можете удалить существующие копии, чтобы очистить место на диске (на самих файлах удаление копий не отразится). Для этого выберите необходимую копию и нажмите кнопку .

Восстановление файлов

В случае если ваши файлы были повреждены, вы можете восстановить их копии за определенную дату. Для этого:

1. Выберите необходимую копию (дата сохранения копии указана в столбце слева) и нажмите кнопку .
2. В открывшемся окне укажите путь к папке, куда будут восстановлены файлы.



13. Инструменты

В этом окне предоставляется доступ к дополнительным инструментам управления продуктом Dr.Web.

Чтобы перейти в группу настроек Инструменты

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Инструменты**.

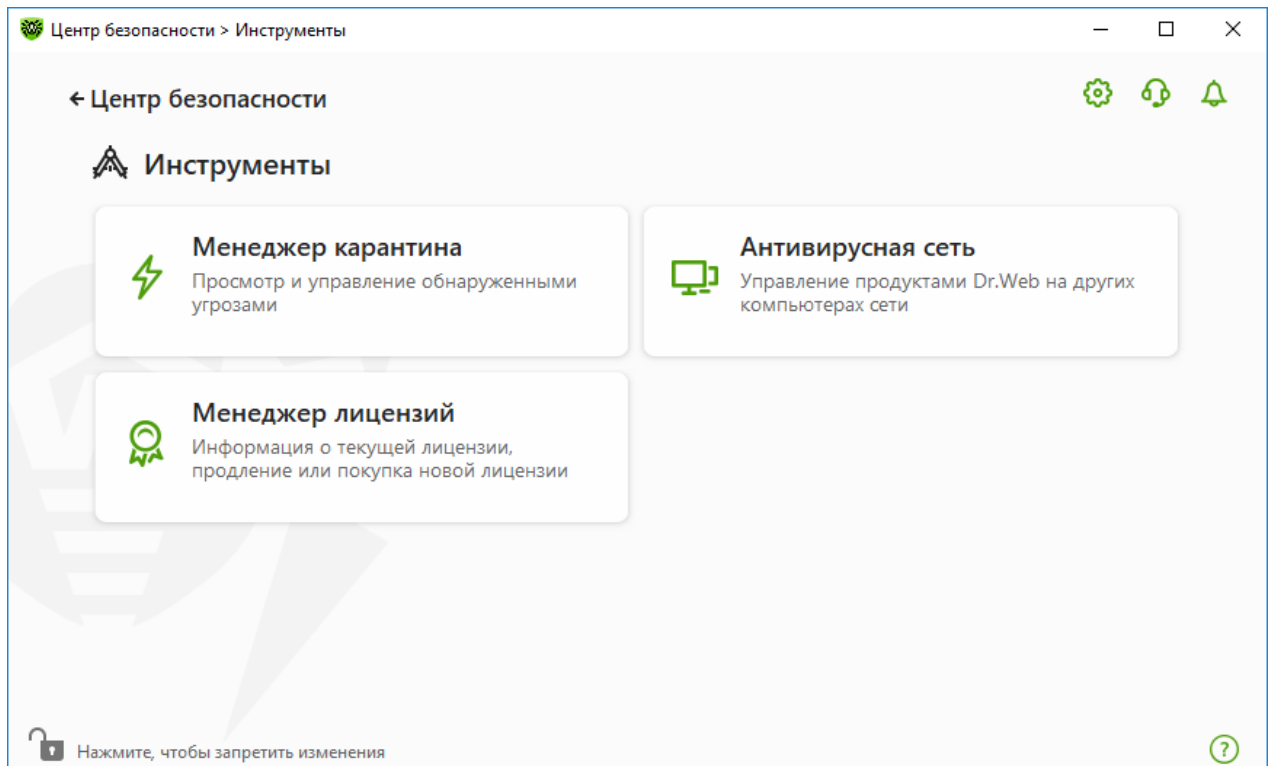


Рисунок 55. Окно Инструменты

Для перехода к необходимому инструменту нажмите соответствующую плитку.

В этом разделе:

- [Менеджер карантина](#) — список изолированных файлов и возможность их восстановления.
- [Антивирусная сеть](#) — удаленный доступ к продуктам Dr.Web, установленных на других компьютерах внутри вашей сети.
- [Менеджер лицензий](#) — информация о лицензии, получение новой лицензии.



13.1. Менеджер карантина

Менеджер карантина — инструмент, позволяющий управлять изолированными файлами. В карантине содержатся файлы, в которых были обнаружены вредоносные объекты. Также в карантин помещаются резервные копии файлов, обработанных Dr.Web. Менеджер карантина предоставляет возможность удаления, перепроверки и восстановления изолированных файлов.

Чтобы перейти в окно Менеджер карантина

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Инструменты**.
3. Нажмите плитку **Менеджер карантина**.

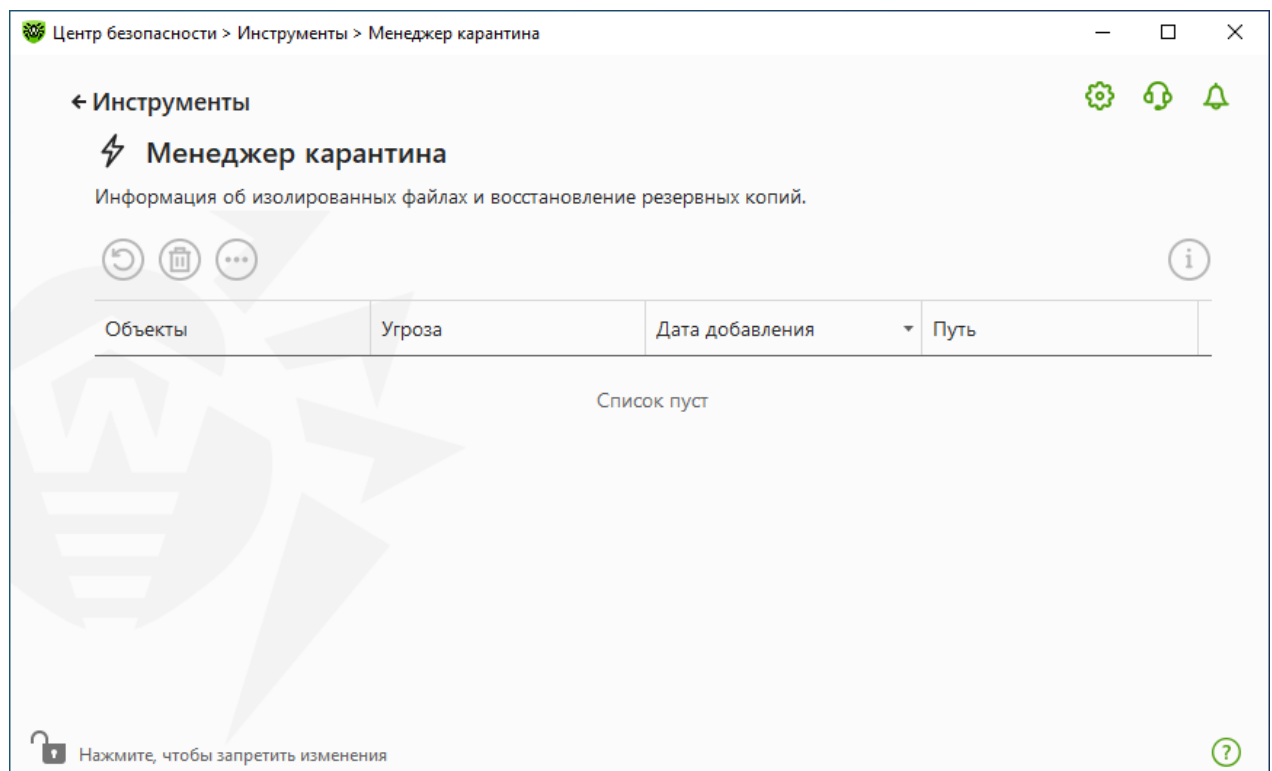


Рисунок 56. Объекты в карантине

В центральной части окна отображается таблица с информацией о состоянии карантина, включающая следующие поля:

- **Объекты** — список имен объектов, находящихся в карантине;
- **Угроза** — классификация вредоносной программы, определяемая Dr.Web при автоматическом перемещении объекта в карантин;
- **Дата добавления** — дата, когда объект был перемещен в карантин;
- **Путь** — полный путь, по которому находился объект до перемещения в карантин.



В окне Менеджера карантина файлы могут видеть только те пользователи, которые имеют к ним доступ. Чтобы отобразить скрытые объекты, необходимо иметь права администратора.

Резервные копии, перемещенные в карантин, по умолчанию не отображаются в таблице. Чтобы видеть их в списке объектов, нажмите кнопку  и в выпадающем списке выберите пункт **Показывать резервные копии**.

Работа с объектами в карантине

В [режиме администратора](#) для каждого объекта доступны следующие кнопки управления:

- Кнопка  (**Восстановить**) — переместить один или несколько выбранных объектов в нужную папку.



Используйте данную функцию только в том случае, если вы уверены, что объект безопасен.

- Кнопка  (**Удалить**) — удалить один или несколько выбранных объектов из карантина и из системы.

Эти действия доступны также в контекстном меню при нажатии правой кнопкой мыши на один или несколько выбранных объектов.

Чтобы удалить сразу все объекты из карантина, нажмите кнопку  и в выпадающем списке выберите пункт **Удалить все**.

Вы можете просмотреть подробную информацию об объекте, добавленном в карантин. Для этого выберите необходимую строку и нажмите .

Дополнительно

Для настройки опций хранения и автоматического удаления записей в карантине перейдите в [настройки Менеджера карантина](#).

13.2. Антивирусная сеть

Этот инструмент позволяет управлять программами Антивирус Dr.Web для Windows, Dr.Web Server Security Suite, Dr.Web Katana и Dr.Web Security Space в рамках одной версии продукта на других компьютерах в пределах одной локальной сети.



Чтобы перейти в окно Антивирусная сеть

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. В открывшемся окне нажмите плитку **Инструменты**.
3. Нажмите плитку **Антивирусная сеть**.

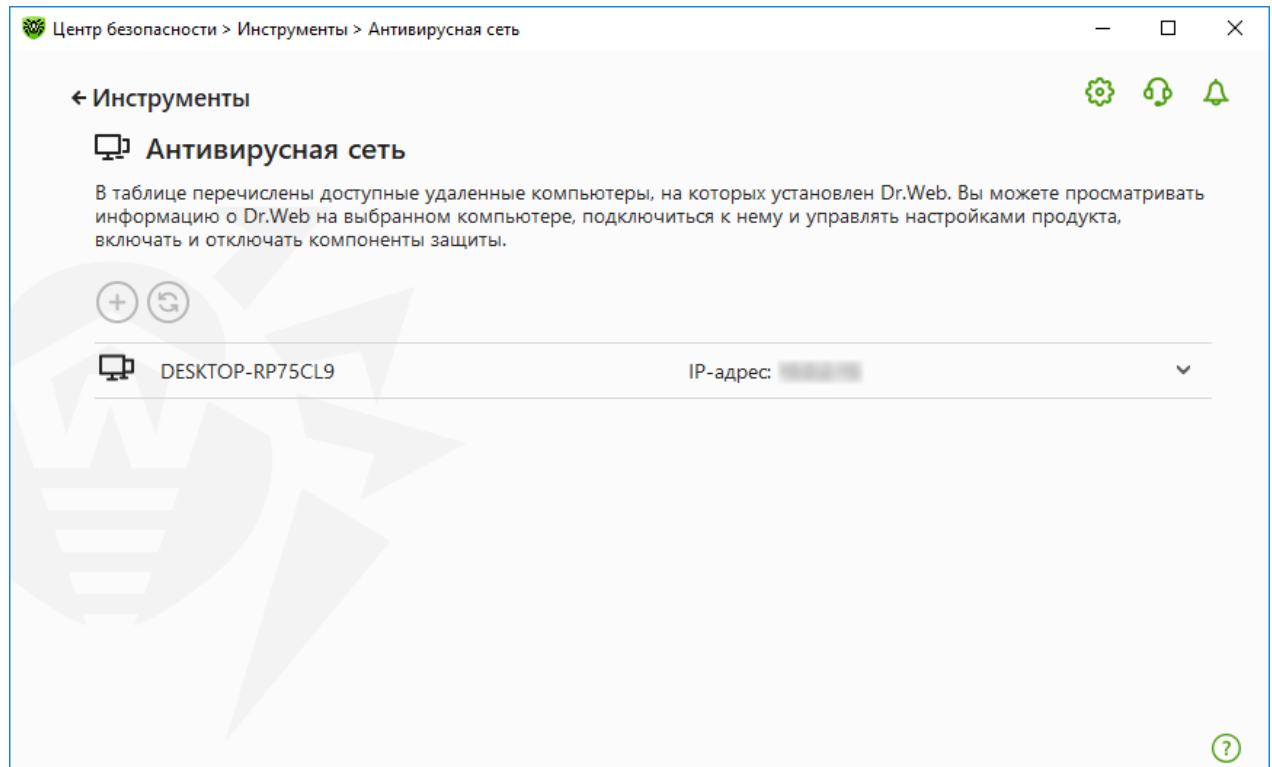


Рисунок 57. Компьютеры антивирусной сети

Компьютеры в локальной сети отображаются в списке только в том случае, если в установленном на них продукте Dr.Web разрешено удаленное управление. Вы можете разрешить подключение к Dr.Web на вашем компьютере в окне [настроек Антивирусной сети](#).

Если необходимый компьютер не отображается в сети, попробуйте добавить его вручную. Для этого нажмите кнопку  и введите IP-адрес в формате IPv4 или IPv6.



Если на станции отключен какой-либо из компонентов, появляется индикация в виде восклицательного знака.



Параметры работы Антивирусной сети

В ходе работы антивирусной сети используются multicast и UDP-запросы со следующими параметрами:

Параметры для multicast:

- IP-адрес: 239.194.75.48 или ff08::28 для IPv4 и IPv6 соответственно
- Порт: 55566
- Интервал опроса: 2000 мс

Параметры для UDP-запроса:

- Порт: 55566
- Интервал опроса: 2000 мс

Чтобы подключиться к удаленному антивирусу

1. Выберите нужный компьютер из списка. В раскрывшейся строке отобразится подробная информация о статусе компонентов на станции и о последнем обновлении.
2. Нажмите кнопку **Подключиться**.
3. Введите код, [заданный](#) в настройках удаленного антивируса. В области уведомлений Windows вашего компьютера появится значок удаленного антивируса , а также будет показано уведомление об успешном подключении.



Вы можете установить только одно соединение с удаленным продуктом Dr.Web. При наличии установленного соединения кнопка **Подключиться** недоступна.

Вы можете просматривать статистику, включать и отключать модули, а также изменять их параметры. Антивирусная сеть, Карантин и Защита от потери данных недоступны.

Также вам доступен пункт **Отсоединиться**, при выборе которого завершается установленное соединение с удаленным антивирусом.

13.3. Менеджер лицензий

Этот инструмент позволяет просмотреть информацию обо всех [лицензиях](#) Dr.Web, хранящихся на вашем компьютере, а также изменить текущую лицензию, продлить ее или купить новую и активировать для использования.

Чтобы перейти в окно Менеджер лицензий из Центра безопасности

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.



2. В открывшемся окне нажмите плитку **Инструменты**.
3. Нажмите плитку **Менеджер лицензий**.

Чтобы перейти в окно Менеджер лицензий из Меню программы

1. Откройте [меню](#) Dr.Web .
2. Выберите пункт **Лицензия**.

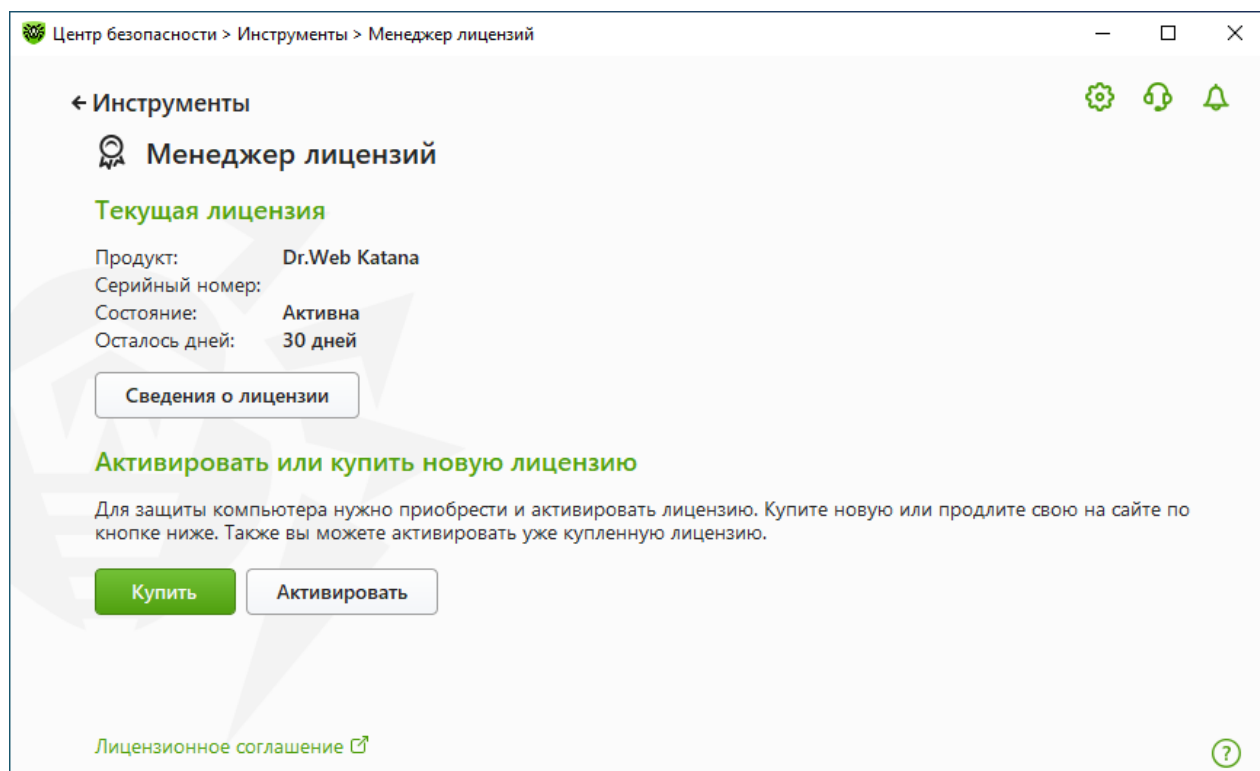


Рисунок 58. Менеджер лицензий

Чтобы посмотреть подробную информацию о текущей лицензии, нажмите кнопку **Сведения о лицензии**.

Чтобы просмотреть информацию о лицензии, которая на данный момент не является текущей

1. Нажмите кнопку **Сведения о лицензии**. Откроется окно Сведений о лицензии.
2. В выпадающем списке выберите подходящую лицензию.

Если действие лицензии распространяется на несколько продуктов, список продуктов доступен в раскрывающемся списке по ссылке **Еще**.



Если активировано несколько действующих лицензий одновременно, срок действия каждой лицензии будет истекать. Чтобы этого не произошло, при активации новой лицензии укажите серийные номера предыдущих активированных лицензий. Тогда сроки действия лицензий суммируются.



Чтобы удалить лицензию

1. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
2. Нажмите кнопку **Сведения о лицензии**. Откроется окно Сведений о лицензии.
3. Выберите из выпадающего списка лицензию, которую вы хотите удалить, и нажмите кнопку . Обратите внимание, что последнюю действующую лицензию удалить нельзя.

Чтобы назначить текущую лицензию

1. Убедитесь, что Dr.Web работает в [режиме администратора](#) (замок в нижней части программы «открыт» ). В противном случае нажмите на замок .
2. Нажмите кнопку **Сведения о лицензии**. Откроется окно Сведений о лицензии.
3. Выберите из выпадающего списка лицензию, которую вы хотите назначить текущей, и нажмите кнопку .

При нажатии кнопки **Купить** программа откроет страницу на сайте компании «Доктор Веб», где вы можете купить или продлить лицензию.

- Если у вас нет активированной лицензии, программа откроет страницу покупки лицензии. Следуйте инструкциям на сайте, чтобы приобрести новую лицензию и активировать ее.
- Если у вас уже есть активированная лицензия, программа откроет страницу продления лицензии, на которую будут переданы параметры используемой лицензии. Следуйте инструкциям на сайте, чтобы приобрести и активировать продление действия лицензии. Подробнее о продлении см. в разделе [Продление лицензии](#).

При нажатии кнопки **Активировать** откроется окно, в котором вы можете [активировать новую лицензию](#).

Дополнительно

Ссылка [Лицензионное соглашение](#)  открывает текст соглашения на сайте компании «Доктор Веб».



14. Статистика работы компонентов

У вас есть возможность просматривать статистику работы основных компонентов Dr.Web.

Чтобы перейти к просмотру статистики по важным событиям в работе компонентов защиты

1. Откройте [меню](#) Dr.Web  и выберите пункт **Центр безопасности**.
2. В открывшемся окне выберите вкладку **Статистика**.
3. Откроется окно просмотра статистики, из которого доступны отчеты для следующих групп:
 - [Подробный отчет](#)
 - [Угрозы](#)

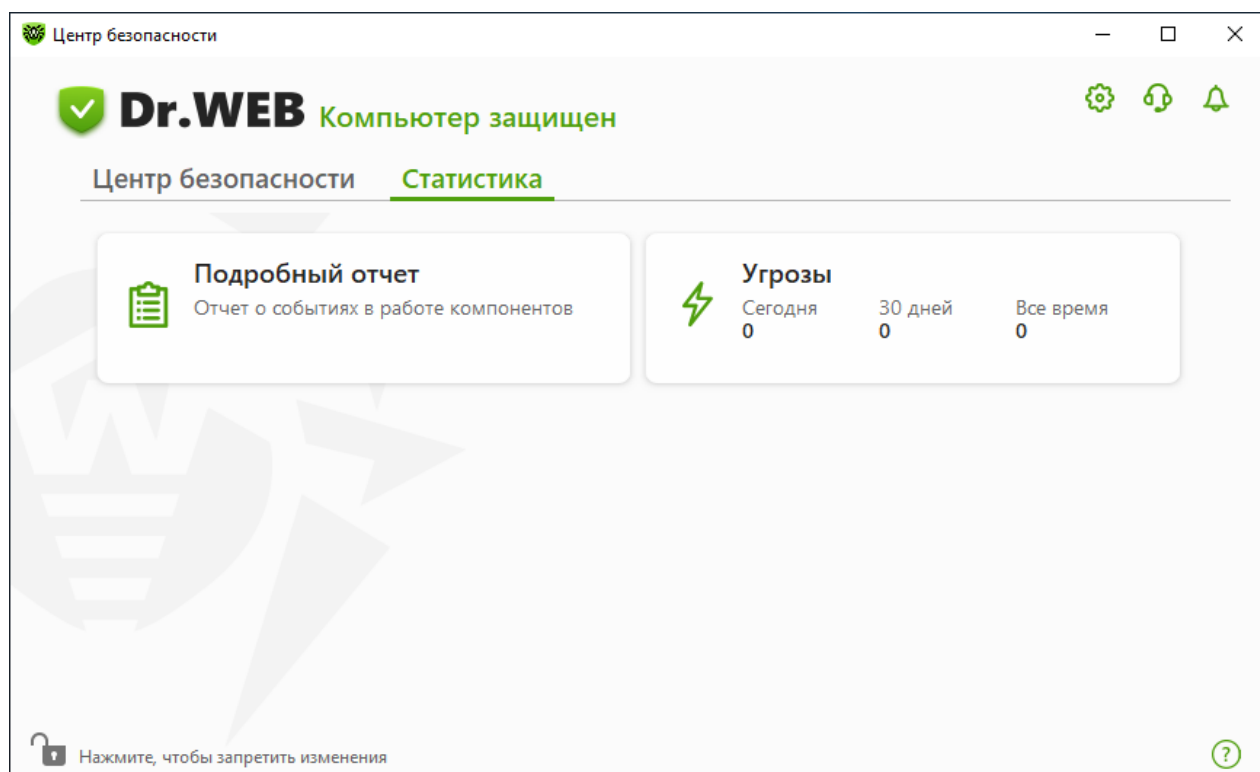


Рисунок 59. Статистика работы компонентов

4. Выберите группу для просмотра отчетов.

Подробный отчет

В этом окне собирается подробная информация обо всех событиях за все время работы.



Центр безопасности > Статистика > Подробный отчет

← Статистика

Подобранный отчет

Дата	Компонент	Событие
1/21/2025 8:44 PM	Модуль обновлен...	Обновление завершено
1/21/2025 8:10 PM	Модуль обновлен...	Обновление завершено
1/21/2025 7:28 PM	Модуль обновлен...	Обновление завершено
1/21/2025 7:01 PM	Модуль обновлен...	Обновление завершено
1/21/2025 6:54 PM	Модуль обновлен...	Обновление завершено
1/21/2025 6:00 PM	Модуль обновлен...	Обновление завершено
1/21/2025 5:28 PM	Модуль обновлен...	Обновление завершено
1/21/2025 4:59 PM	Модуль обновлен...	Обновление завершено
1/21/2025 4:27 PM	Модуль обновлен...	Обновление завершено

Нажмите, чтобы запретить изменения

Рисунок 60. Окно подробного отчета

В отчете фиксируются следующие сведения:

- **Дата** — дата и время события;
- **Компонент** — компонент или модуль, к которому относится событие;
- **Событие** — краткое описание события.

По умолчанию отображаются все события за все время.

Для работы с объектами в таблице используются [элементы управления](#) , , .

Для отбора событий можно воспользоваться [дополнительными фильтрами](#).

Угрозы

В основном окне просмотра статистики на плитке **Угрозы** собрана информация о количестве угроз за определенный промежуток времени.



При выборе этой опции откроется окно **Подробный отчет** с предустановленными фильтрами по всем угрозам.

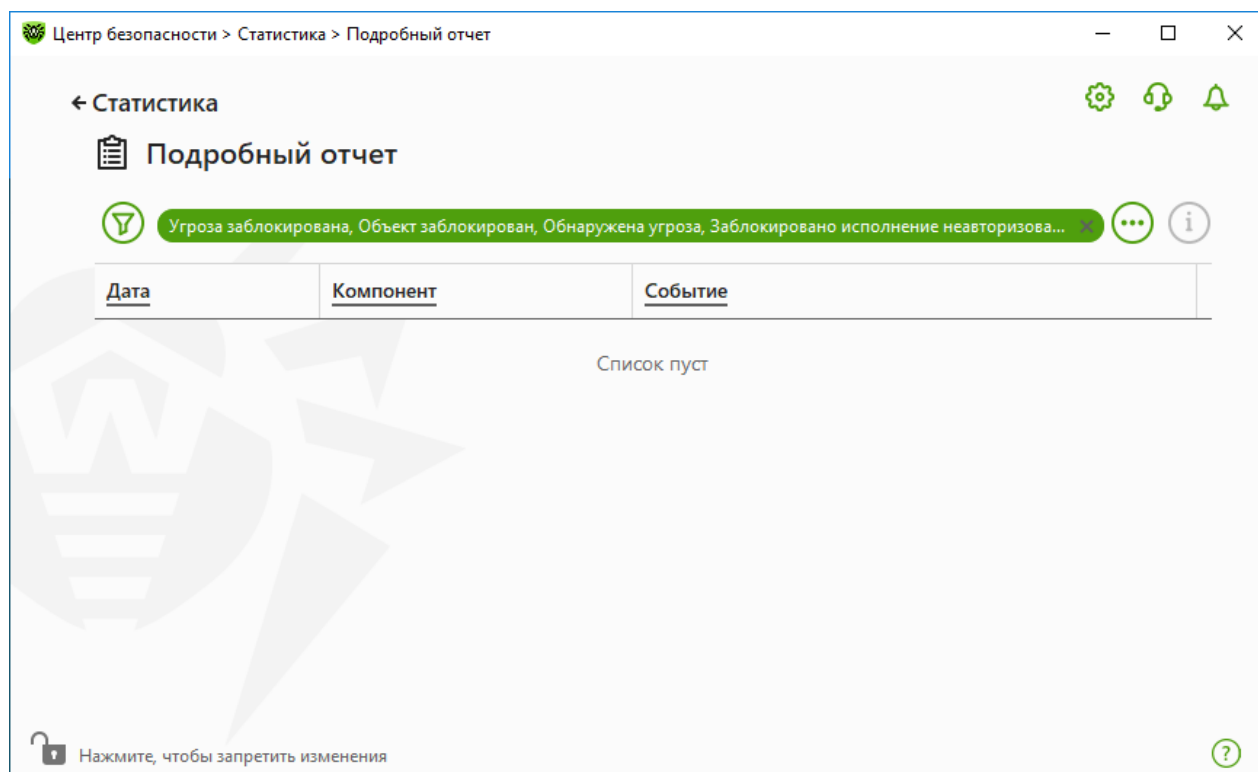


Рисунок 61. Окно статистики по угрозам

В отчете фиксируются следующие сведения:

- **Дата** — дата и время обнаружения угрозы;
- **Компонент** — компонент, обнаруживший угрозу;
- **Событие** — краткое описание события.

По умолчанию отображаются все события за все время.

Для работы с объектами в таблице используются [элементы управления](#) , , .

Для отбора событий можно воспользоваться [дополнительными фильтрами](#).

Фильтры

Чтобы посмотреть в списке только те события, которые соответствуют определенным параметрам, воспользуйтесь фильтрами. Для всех отчетов имеются предустановленные фильтры, которые доступны по нажатию . Также вы можете создавать собственные фильтры событий.



Кнопки управления элементами в таблице:

- При нажатии кнопки  доступны следующие действия:
 - Выбор предустановленного фильтра за установленный период времени или фильтра по событию обновления.
 - Сохранение текущего пользовательского фильтра. Также возможно удаление уже созданного пользовательского фильтра.
 - Удаление всех установленных на данный момент фильтров.
- При нажатии кнопки  доступны следующие действия:
 - **Копировать выделенное** — позволяет скопировать выделенную строку (строки) в буфер обмена.
 - **Экспортировать выделенное** — позволяет экспортировать выделенную строку (строки) в заданную папку в формате .csv.
 - **Экспортировать все** — позволяет экспортировать все строки таблицы в заданную папку в формате .csv.
 - **Удалить выделенное** — позволяет удалить выделенное событие (события).
 - **Удалить все** — позволяет удалить все события из таблицы статистики.
- При нажатии кнопки  отображается подробная информация о событии. Доступна при выборе какой-либо строки. Повторное нажатие этой кнопки скроет подробные данные о событии.

Чтобы задать пользовательский фильтр

1. Для сортировки по определенному параметру нажмите на заголовок необходимого столбца:
 - Сортировка по дате. Вы можете выбрать один из предустановленных периодов, указанных в левой части окна, или задать свой. Чтобы задать необходимый период, выберите в календаре дату начала и дату окончания периода, либо укажите даты в строке **Период**. Также доступна сортировка по дате по возрастанию или убыванию.

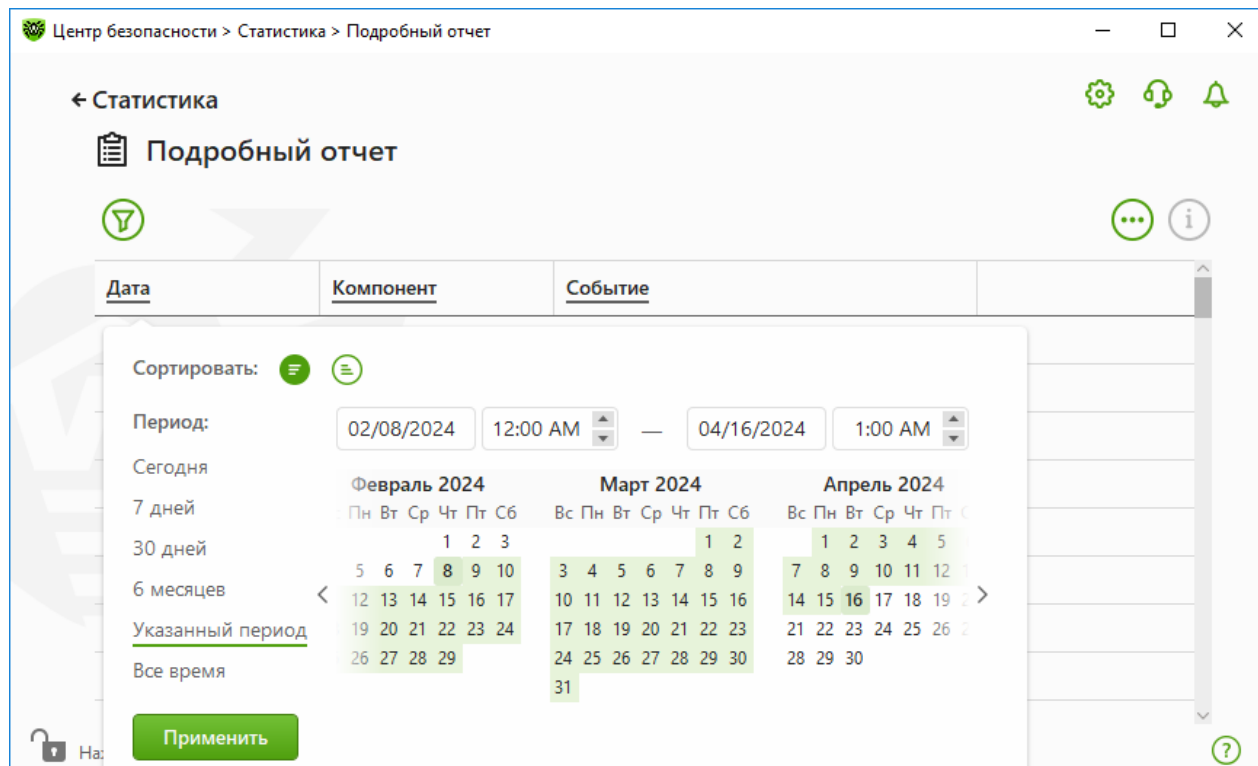


Рисунок 62. Сортировка по дате

- Сортировка по компоненту. Вы можете отметить те компоненты, информация от которых будет отображаться в отчете, либо отсортировать записи по возрастанию или убыванию.
 - Сортировка по событию. Вы можете отметить события для отображения в отчете либо отсортировать записи по возрастанию или убыванию.
2. После выбора параметров фильтрации нажмите **Применить**. Выбранные элементы будут отображаться над таблицей.
 3. Чтобы сохранить фильтр, нажмите  и выберите **Сохранить фильтр**.
 4. В открывшемся окне укажите название нового фильтра. Нажмите **Сохранить**.



15. Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

1. Ознакомьтесь с последними версиями описаний и руководств по адресу <https://download.drweb.com/doc/>.
2. Прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/.
3. Посетите форумы компании «Доктор Веб» по адресу <https://forum.drweb.com/>.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

1. Заполните веб-форму в соответствующей секции раздела <https://support.drweb.com/>.
2. Позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу <https://company.drweb.com/contacts/offices/>.

15.1. Помощь в решении проблем

При обращении вам может потребоваться сформировать отчет о вашей операционной системе и работе Dr.Web.

Чтобы создать отчет при помощи Мастера отчетов

1. Откройте [меню](#) Dr.Web  и выберите пункт **Поддержка**.
2. В открывшемся окне нажмите кнопку **Перейти к Мастеру отчетов**.

Также вы можете открыть это окно, нажав на кнопку  в правой верхней части окна **Центр безопасности**.

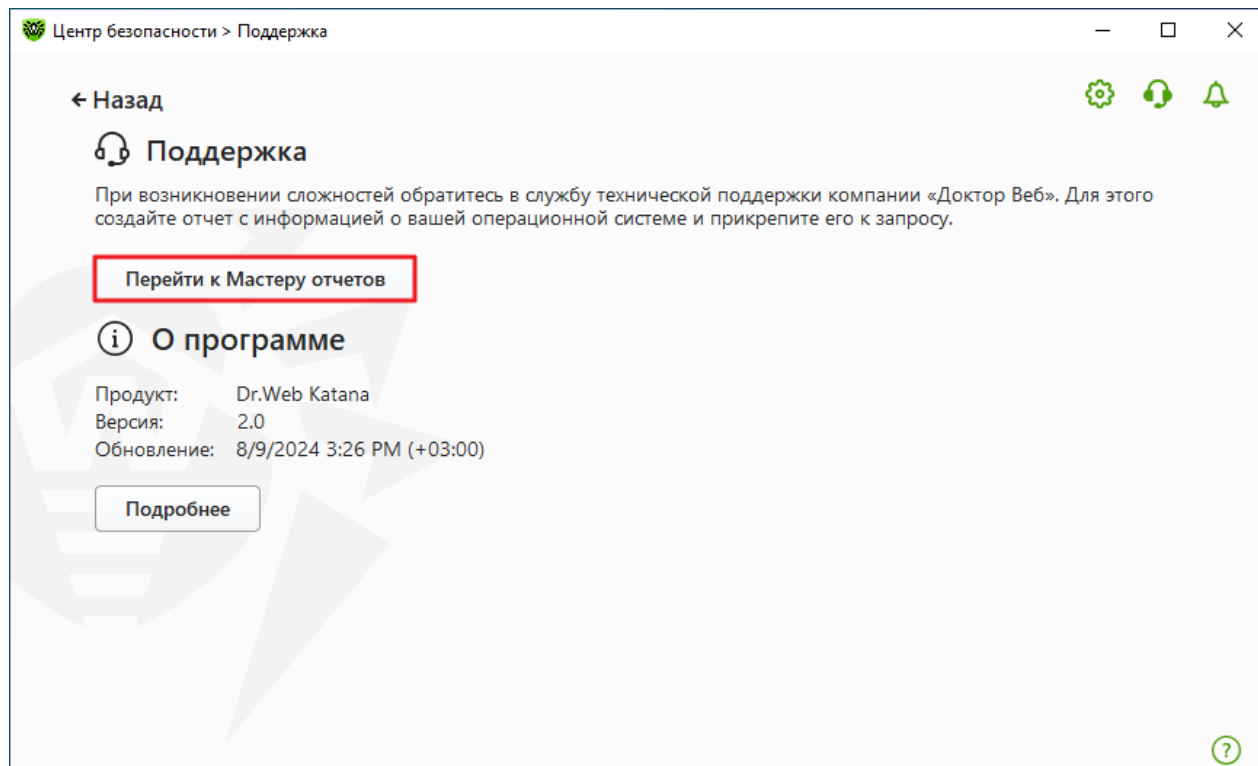


Рисунок 63. Поддержка

3. В открывшемся окне нажмите кнопку **Создать отчет**.

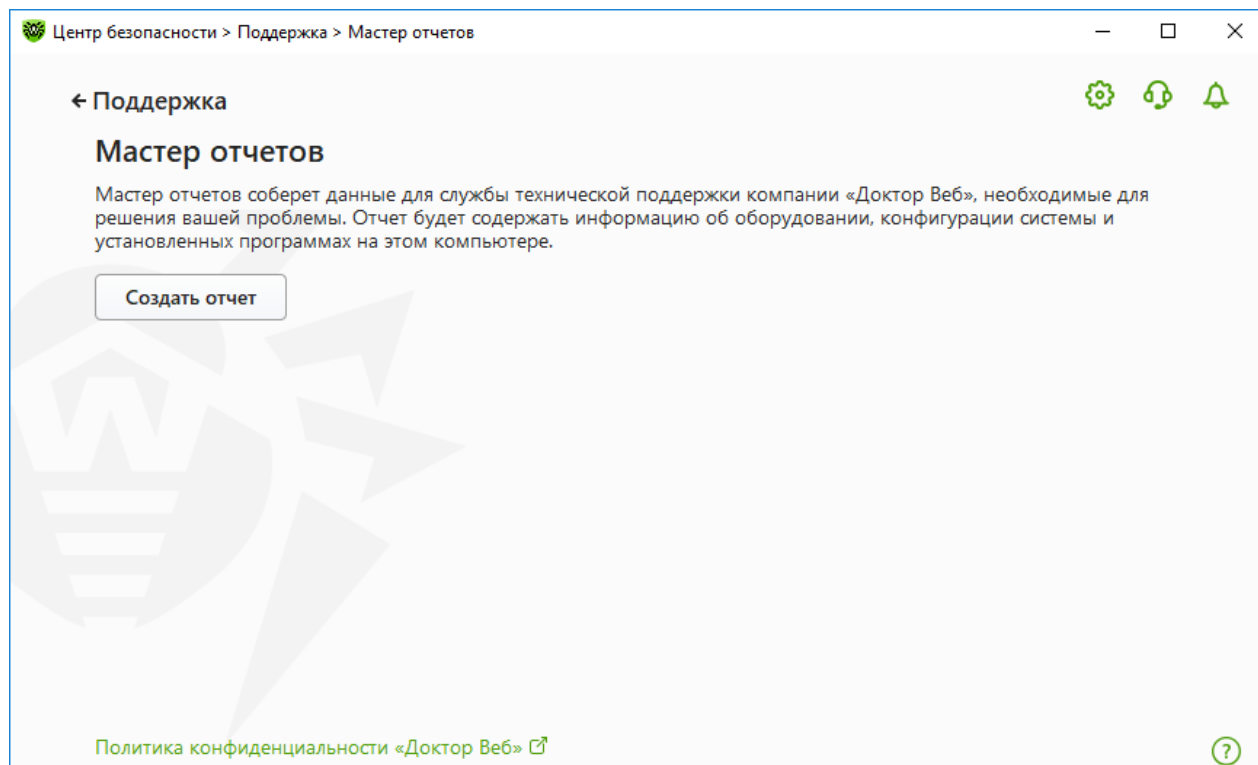


Рисунок 64. Создание отчета для технической поддержки

4. Начнется создание отчета.



Создание отчета при помощи командной строки

Чтобы сформировать отчет, воспользуйтесь следующей командой:

/auto, например: dwsysinfo.exe /auto

Также вы можете использовать команду:

/auto /report:[<полный_путь_к_файлу_отчета>], например: dwsysinfo.exe /auto /report:C:\report.zip

Отчет будет сохранен в виде архива в папке Doctor Web, расположенной в папке профиля пользователя %USERPROFILE%. Вы можете получить доступ к архиву, нажав кнопку **Открыть папку** после завершения создания архива. Отчет защищен паролем virus.

Информация, которая включается в отчет

В отчет включается следующая информация:

1. Техническая информация об операционной системе:

- общие сведения о компьютере,
- информация о запущенных процессах,
- информация о запланированных заданиях,
- информация о службах, драйверах,
- информация о браузере по умолчанию,
- информация об установленных приложениях,
- информация о политиках ограничений,
- информация о файле HOSTS,
- информация о серверах DNS,
- записи системного журнала событий;
- перечень системных каталогов;
- ветви реестра;
- провайдеры Winsock;
- сетевые соединения;
- отчеты отладчика Dr. Watson;
- индекс производительности.

2. Информация об установленном продукте Dr.Web:

- тип и версия установленного продукта Dr.Web;
- информация о составе установленных компонентов; сведения о модулях Dr.Web;



- настройки и параметры конфигурации продукта Dr.Web;
- информация о лицензии;
- журналы работы Dr.Web.

Информация о работе Dr.Web находится в Журнале событий операционной системы Windows, в разделе **Журналы приложений и служб** → **Doctor Web**.

15.2. О программе

Блок **О программе** содержит информацию о:

- версии продукта;
- дате и времени последнего обновления.

Информацию о версии установленных компонентов вы можете найти в окне **О программе Dr.Web**.

Чтобы перейти к этому окну

1. Откройте основное меню  и выберите пункт **Поддержка**.
2. В открывшемся окне нажмите кнопку **Подробнее**.

Также вы можете открыть это окно, нажав на кнопку  в правой верхней части окна **Центр безопасности**.

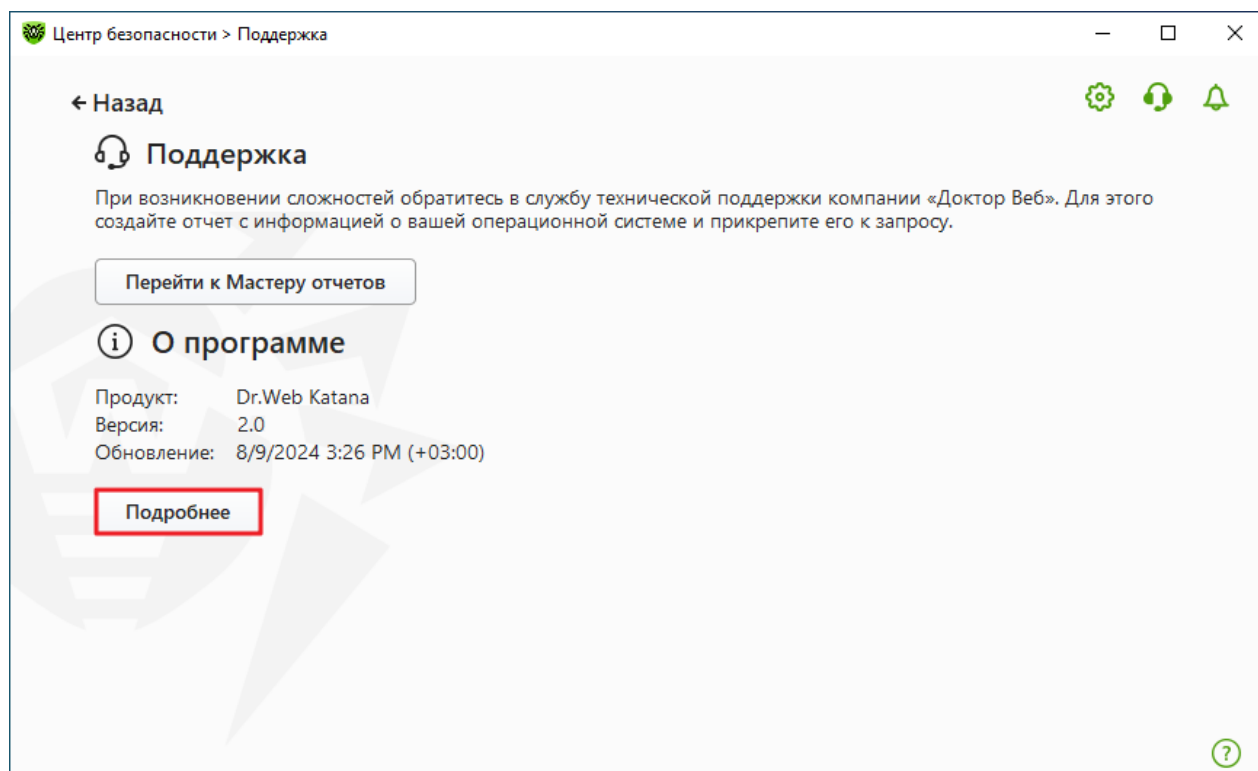


Рисунок 65. Доступ к окну О программе Dr.Web



16. Приложение А. Дополнительные параметры командной строки

Параметры командной строки используются для задания параметров программам, которые могут быть запущены путем открытия на выполнение исполняемого файла. Это относится к Модулю автоматического обновления.

Ключи начинаются с символа «/» и, как и остальные параметры командной строки, разделяются пробелами.

16.1. Параметры для Модуля обновления

Общие параметры:

Параметр	Описание
-h [--help]	Вывести на экран краткую справку о работе с программой.
-v [--verbosity] arg	Уровень детализации журнала: <code>error</code> (только ошибки), <code>info</code> (стандартный), <code>debug</code> (отладочный).
--rotate arg	Ротация журнала в формате <i><количество файлов>, <размер> <единица измерения></i> (к — килобайт, м — мегабайт, г — гигабайт).
-d [--data-dir] arg	Папка, в которой размещены репозиторий и настройки.
--log-dir arg	Папка, в которой будет сохранен журнал.
-r [--repo-dir] arg	Папка репозитория (по умолчанию <i><data_dir>/repo</i>).
-t [--trace]	Включить трассировку.
-c [--command] arg (=update)	Выполняемая команда: <code>update</code> — обновить, <code>uninstall</code> — удалить, <code>exec</code> — выполнить, <code>keyupdate</code> — обновить ключ, <code>download</code> — скачать, <code>mirror</code> — создать зеркало обновлений.
-z [--zone] arg	Список зон, который будет использоваться вместо заданных в конфигурационном файле.

Параметры команды обновления (update):

Параметр	Описание
-p [--product] arg	Название продукта. Если название указано, то будет произведено обновление только этого продукта. Если продукт не указан и не



Параметр	Описание
	указаны конкретные компоненты, будет произведено обновление всех продуктов. Если указаны компоненты, будет произведено обновление указанных компонентов.
-n [--component] arg	Перечень компонентов, которые необходимо обновить до определенной модификации. Формат: <i><name></i> , <i><target revision></i> .
-x [--selfrestart] arg (=yes)	Перезапуск после обновления Модуля обновления. По умолчанию значение <i>yes</i> . Если указано значение <i>no</i> , то выводится предупреждение о необходимости перезапуска.
--geo-update	Получить список IP-адресов <i>update.drweb.com</i> перед обновлением.
--type arg (=normal)	Может быть одним из следующих: • <i>reset-all</i> — принудительное обновление всех компонентов; • <i>reset-failed</i> — сбросить все изменения для поврежденных компонентов; • <i>normal-failed</i> — попытаться обновить компоненты, включая поврежденные, до последней либо до указанной версии; • <i>update-revision</i> — обновить компоненты в пределах текущей ревизии; • <i>normal</i> — обновить все компоненты.
-g [--proxy] arg	Прокси-сервер для обновления в формате <i><адрес></i> : <i><порт></i> .
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
--param arg	Передать дополнительные параметры в скрипт. Формат: <i><имя></i> : <i><значение></i> .
-l [--progress-to-console]	Вывести на консоль информацию о загрузке и выполнении скрипта.

Параметры команды удаления (uninstall):

Параметр	Описание
-n [--component] arg	Имя компонента, который необходимо удалить.
-l [--progress-to-console]	Вывести информацию о выполнении команды на консоль.
--param arg	Передать дополнительные параметры в скрипт. Формат: <i><имя></i> : <i><значение></i> .



Параметр	Описание
-e [--add-to-exclude]	Компоненты, которые будут удалены и их обновление производиться не будет.

Параметры команды автоматического обновления ключа (keyupdate):

Параметр	Описание
-m [--md5] arg	Контрольная сумма md5 старого ключевого файла.
-o [--output] arg	Имя файла.
-b [--backup]	Резервное копирование старого ключевого файла, если он существует.
-g [--proxy] arg	Прокси-сервер для обновления в формате <i><адрес>: <порт></i> .
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-l [--progress-to-console]	Вывести на консоль информацию о загрузке ключевого файла.

Параметры команды скачивания (download):

Параметр	Описание
--zones arg	Файл, содержащий список зон.
--key-dir arg	Папка, в которой находится ключевой файл.
-l [--progress-to-console]	Вывести информацию о выполнении команды на консоль.
-g [--proxy] arg	Прокси-сервер для обновления в формате <i><адрес>: <порт></i> .
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-s [--version] arg	Имя версии.
-p [--product] arg	Название продукта, который необходимо скачать.

**Параметры команды создания зеркала обновлений (mirror):**

Параметр	Описание
--zones arg	Файл, содержащий список зон.
--key-dir arg	Папка, в которой находится ключевой файл.
-g [--proxy] arg	Прокси-сервер для обновления в формате <i><адрес>: <порт></i> .
-u [--user] arg	Имя пользователя прокси-сервера.
-k [--password] arg	Пароль пользователя прокси-сервера.
-s [--version] arg	Имя версии.

16.2. Коды возврата для Модуля обновления

Возможные значения кода возврата и соответствующие им события следующие:

Код возврата	Событие
0	Ошибок нет.
4	Неверные параметры командной строки.
6	Необходим перезапуск обновления.
7	Обновление уже идет.
8	Обновления для указанных продуктов или компонентов не требуются.
9	Ошибка подключения к серверу.
10	Не удалось получить информацию о ревизии компонентов.
11	Список зон обновлений пуст.
12	Лицензия заблокирована.
13	Лицензия отсутствует.
16	Нет информации о лицензии.



17. Приложение Б. Угрозы и способы их обезвреживания

С развитием компьютерных технологий и сетевых решений все большее распространение получают различные вредоносные программы, направленные на то, чтобы так или иначе нанести вред пользователям. Их развитие началось еще в эпоху зарождения вычислительной техники, и параллельно развивались средства защиты от них. Тем не менее, до сих пор не существует единой классификации всех возможных угроз, что связано, в первую очередь, с непредсказуемым характером их развития и постоянным совершенствованием применяемых технологий.

Вредоносные программы могут распространяться через интернет, локальную сеть, электронную почту и съемные носители информации. Некоторые рассчитаны на неосторожность и неопытность пользователя и могут действовать полностью автономно, другие являются лишь инструментами под управлением компьютерных взломщиков и способны нанести вред даже надежно защищенным системам.

В данной главе представлены описания всех основных и наиболее распространенных типов вредоносных программ, на борьбу с которыми в первую очередь и направлены разработки компании «Доктор Веб».

17.1. Виды компьютерных угроз

Под термином «угроза» в данной классификации следует понимать любое программное средство, косвенно или напрямую способное нанести ущерб компьютеру, сети, информации или правам пользователя (то есть вредоносные и прочие нежелательные программы). В более широком смысле термин «угроза» может означать любую потенциальную опасность для компьютера или сети (то есть ее уязвимость, которая может быть использована для проведения хакерских атак).

Все типы программ, описанные ниже, потенциально обладают способностью подвергнуть опасности данные пользователя или их конфиденциальность. Программы, которые не скрывают своего присутствия в системе (например, некоторые программы для рассылки спама или анализаторы трафика), обычно не принято причислять к компьютерным угрозам, хотя при определенных обстоятельствах они также могут нанести вред пользователю.

Компьютерные вирусы

Данный тип компьютерных угроз характеризуется способностью внедрять свой код в исполняемый код других программ. Такое внедрение называется *инфицированием*. В большинстве случаев инфицированный файл сам становится носителем вируса, а внедренный код не обязательно полностью соответствует оригиналу. Большая часть вирусов создается для повреждения или уничтожения данных.



В компании «Доктор Веб» вирусы делят по типу файлов, которые они инфицируют:

- *Файловые вирусы* инфицируют файлы операционной системы (обычно исполняемые файлы и динамические библиотеки) и активизируются при обращении к инфицированному файлу.
- *Макро-вирусы* инфицируют документы, которые используют программы из пакета Microsoft Office (и другие программы, которые используют макросы, написанные, например, на языке Visual Basic). *Макросы* – это встроенные программы, написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, в Microsoft Word макросы могут запускаться при открытии, закрытии или сохранении документа).
- *Скрипт-вирусы* пишутся на языках сценариев (скриптов) и в большинстве случаев инфицируют другие файлы сценариев (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение сценариев, пользуясь уязвимыми сценариями в веб-приложениях.
- *Загрузочные вирусы* инфицируют загрузочные сектора дисков и разделов, а также главные загрузочные сектора жестких дисков. Они занимают очень мало памяти и остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными защитными механизмами против обнаружения. Методы защиты от обнаружения постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты. Вирусы можно разделить по принципу защиты от обнаружения:

- *Шифрованные вирусы* шифруют свой код при каждом новом инфицировании, что затрудняет его обнаружение в файле, памяти или загрузочном секторе. Каждый экземпляр такого вируса содержит только короткий общий фрагмент (процедуру расшифровки), который можно выбрать в качестве сигнатуры.
- *Полиморфные вирусы* используют помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у такого вируса байтовых сигнатур.
- *Стелс-вирусы* (вирусы-невидимки) предпринимают специальные действия для маскировки своей деятельности с целью сокрытия своего присутствия в инфицированных объектах. Такой вирус снимает характеристики объекта перед его инфицированием, а затем передает старые данные при запросе операционной системы или программы, ищущей измененные файлы.

Вирусы также можно классифицировать по языку, на котором они написаны (большинство пишутся на языке ассемблера, но имеются также и вирусы, написанные на высокоуровневых языках программирования, языках сценариев и т. д.) и по инфицируемым ими операционным системам.



Компьютерные черви

В последнее время вредоносные программы типа «компьютерный червь» стали гораздо более распространены, чем вирусы и прочие вредоносные программы. Как и вирусы, такие программы способны создавать свои копии, но при этом они не инфицируют другие объекты. Червь проникает на компьютер из сети (чаще всего как вложение в сообщениях электронной почты или через интернет) и рассылает свои функциональные копии на другие компьютеры. Для начала распространения черви могут использовать как действия пользователя, так и автоматический режим выбора и атаки компьютера.

Черви не обязательно целиком состоят из одного файла (тела червя). У многих червей есть так называемая инфекционная часть (шелл-код), которая загружается в оперативную память компьютера и «догружает» по сети непосредственно само тело червя в виде исполняемого файла. Пока в системе нет тела червя, от него можно избавиться перезагрузкой компьютера (при которой происходит сброс оперативной памяти). Если же в системе оказывается тело червя, то справиться с ним может только антивирус.

За счет интенсивного распространения черви способны вывести из строя целые сети, даже если они не несут никакой полезной нагрузки (не наносят прямой вред системе).

В компании «Доктор Веб» червей делят по способу (среде) распространения:

- *Сетевые черви* распространяются посредством различных сетевых протоколов и протоколов обмена файлами.
- *Почтовые черви* распространяются посредством почтовых протоколов (POP3, SMTP и т. д.).
- *Чат-черви* распространяются, используя популярные программы для пересылки мгновенных сообщений (ICQ, IM, IRC и т. д.).

Троянские программы

Этот тип вредоносных программ не способен к саморепликации. Троянские программы подменяют какую-либо из часто запускаемых программ и выполняют ее функции (или имитируют исполнение этих функций), одновременно производя какие-либо вредоносные действия (повреждение и удаление данных, пересылка конфиденциальной информации и т. д.), либо делая возможным несанкционированное использование компьютера злоумышленником, например, для нанесения вреда третьим лицам.

Эти программы обладают схожими с вирусом маскировочными и вредоносными функциями и даже могут быть модулем вируса, но, как правило, троянские программы распространяются как отдельные исполняемые файлы (выкладываются на файловые сервера, записываются на носители информации или пересылаются в виде вложений в сообщениях электронной почты), которые запускаются либо самим пользователем, либо определенным процессом системы.



Классифицировать троянские программы очень непросто, во-первых, потому что они зачастую распространяются вирусами и червями, во-вторых, вредоносные действия, которые могут выполнять другие типы угроз, принято приписывать только троянским программам. Ниже приведен список некоторых типов троянских программ, которые в компании «Доктор Веб» выделяют в отдельные классы:

- *Бэкдоры* – это троянские программы, которые позволяют получать привилегированный доступ к системе в обход существующего механизма предоставления доступа и защиты. Бэкдоры не инфицируют файлы; они прописывают себя в реестре, модифицируя ключи.
- *Руткиты* предназначены для перехвата системных функций операционной системы с целью сокрытия своего присутствия в системе. Кроме того, руткит может маскировать процессы других программ, различные ключи реестра, папки, файлы. Руткит распространяется как самостоятельная программа или как дополнительный компонент в составе другой вредоносной программы. По принципу своей работы руткиты условно разделяют на две группы: руткиты, работающие в режиме пользователя (перехват функций библиотек пользовательского режима) (*User Mode Rootkits – UMR*), и руткиты, работающие в режиме ядра (перехват функций на уровне системного ядра, что значительно усложняет обнаружение и обезвреживание) (*Kernel Mode Rootkits – KMR*).
- *Клавиатурные перехватчики (кейлоггеры)* используются для сбора данных, которые пользователь вводит при помощи клавиатуры. Целью таких действия является кража личной информации (например, сетевых паролей, логинов, номеров банковских карт и т. д.).
- *Кликеры* переопределяют ссылки при нажатии на них и таким образом перенаправляют пользователей на определенные (возможно, вредоносные) сайты. Обычно пользователь перенаправляется с целью увеличения рекламного трафика веб-сайтов или для организации распределенных атак отказа в обслуживании (DDoS-атак).
- *Прокси-трояны* предоставляют злоумышленнику анонимный выход в интернет через компьютер жертвы.

Кроме перечисленных выше, троянские программы могут выполнять и другие вредоносные действия, например, изменять стартовую страницу в веб-браузере или удалять определенные файлы. Однако такие действия могут выполняться и угрозами других типов (например, вирусами и червями).

Программы взлома

Программы взлома созданы с целью помочь взломщику. Наиболее распространенным видом подобных программ являются сканеры портов, которые позволяют обнаруживать уязвимости в межсетевых экранах (файерволах, брандмауэрах) и других компонентах, обеспечивающих безопасность компьютера. Кроме хакеров, такими инструментами могут пользоваться администраторы для проверки надежности своих



сетей. Иногда к программам взлома относят программы, использующие методы социальной инженерии (элементы социотехники).

Рекламные программы

Чаще всего под этим термином понимают программный код, встроенный в различное бесплатное программное обеспечение, при использовании которого пользователю принудительно показывается реклама. Но иногда такой код может скрытно распространяться посредством других вредоносных программ и демонстрировать рекламу, например в веб-браузерах. Зачастую рекламные программы работают на основании данных, собранных шпионскими программами.

Программы-шутки

Это тип вредоносных программ, которые, как и рекламные программы, не наносят прямого вреда системе. Чаще всего они генерируют сообщения о несуществующих ошибках и угрожают действиями, которые могут привести к повреждению данных. Их основной функцией является запугивание пользователя, либо навязчивое его раздражение.

Программы дозвона

Это специальные компьютерные программы, разработанные для сканирования некоего диапазона телефонных номеров для нахождения такого, на который ответит модем. В дальнейшем злоумышленники используют найденные номера для накручивания оплаты за телефон или для незаметного подключения пользователя через модем к дорогостоящим платным телефонным службам.

Потенциально опасные программы

Эти программы не создавались для нанесения вреда, но в силу своих особенностей могут представлять угрозу для безопасности системы. К таким программам относятся не только те, которые могут случайно повредить или удалить данные, но и те, которые могут использоваться хакерами или другими программами для нанесения вреда системе. К потенциально опасным программам можно отнести различные программы удаленного общения и администрирования, FTP-серверы и т. д.

Подозрительные объекты

К подозрительным объектам относятся любые потенциальные угрозы, обнаруженные при помощи эвристического анализа. Такие объекты могут являться любым типом компьютерных угроз (возможно, даже неизвестным для специалистов по информационной безопасности), а могут оказаться безопасными в случае ложного срабатывания. Файлы, содержащие подозрительные объекты, рекомендуется помещать



в карантин, а также отправлять на анализ специалистам антивирусной лаборатории компании «Доктор Веб».

17.2. Действия для обезвреживания угроз

Существует множество различных методов борьбы с компьютерными угрозами. Для надежной защиты компьютеров и сетей продукты компании «Доктор Веб» объединяют в себе эти методы при помощи гибких настроек и комплексного подхода к обеспечению безопасности. Основными действиями для обезвреживания вредоносных программ являются:

1. **Лечение** — действие, применяемое к вредоносным программам, червям и троянам. Оно подразумевает удаление вредоносного кода из зараженных файлов либо удаление функциональных копий вредоносных программ, а также, по возможности, восстановление работоспособности пораженных объектов (т. е. возвращение структуры и функционала программы к состоянию, которое было до заражения).
2. **Перемещение в карантин** — действие, при котором вредоносный объект помещается в специальную папку, где изолируется от остальной системы. Данное действие является предпочтительным при невозможности лечения, а также для всех подозрительных объектов. Копии таких файлов желательно пересылать для анализа в антивирусную лабораторию «Доктор Веб».
3. **Удаление** — эффективное действие для борьбы с компьютерными угрозами. Оно применимо для любого типа вредоносных объектов. Следует отметить, что иногда удаление будет применено к некоторым файлам, для которых было выбрано лечение. Это происходит в случае, когда весь файл целиком состоит из вредоносного кода и не содержит никакой полезной информации. Так, например, под лечением компьютерного червя подразумевается удаление всех его функциональных копий.
4. **Блокировка** — это также действие, позволяющее обезвредить вредоносные программы, при котором, однако, в файловой системе остаются их полноценные копии. Блокируются любые попытки обращения от и к вредоносному объекту.



18. Приложение В. Принципы именования угроз

При обнаружении вредоносного кода компоненты Dr.Web сообщают пользователю средствами интерфейса и заносят в файл отчета имя угрозы, присвоенное ей специалистами компании «Доктор Веб». Эти имена строятся по определенным принципам и отражают конструкцию угрозы, классы уязвимых объектов, среду распространения (ОС и прикладные пакеты) и ряд других особенностей. Знание этих принципов может быть полезно для выявления программных и организационных уязвимостей защищаемой системы. Ниже дается краткое изложение принципов именования угроз; более полная и постоянно обновляемая версия описания доступна по адресу <https://vms.drweb.com/classification/>.

Эта классификация в ряде случаев условна, поскольку конкретные виды угроз могут обладать одновременно несколькими приведенными признаками. Кроме того, она не может считаться исчерпывающей, поскольку постоянно появляются новые виды угроз и, соответственно, идет работа по уточнению классификации.

Полное имя угрозы состоит из нескольких элементов, разделенных точками. При этом некоторые элементы, стоящие в начале полного имени (префиксы) и в конце (суффиксы), являются типовыми в соответствии с принятой классификацией.

Основные префиксы

Префиксы операционной системы

Нижеследующие префиксы применяются для называния вредоносных программ, инфицирующих исполняемые файлы определенных платформ (ОС):

- Win — 16-разрядные программы ОС Windows 3.1;
- Win95 — 32-разрядные программы ОС Windows 95/98/Me;
- WinNT — 32-разрядные и 64-разрядные программы ОС Windows NT/2000/XP/Vista/7/8/8.1/10;
- Win32 — 32-разрядные программы различных сред ОС Windows 95/98/Me и ОС Windows NT/2000/XP/Vista/7/8/8.1/10;
- Win64 — 64-разрядные программы ОС Windows XP/Vista/7/8/8.1/10/11;
- Win32.NET — программы в ОС Microsoft .NET Framework;
- OS2 — программы ОС OS/2;
- Unix — программы различных UNIX-систем;
- Linux — программы ОС Linux;
- FreeBSD — программы ОС FreeBSD;
- SunOS — программы ОС SunOS (Solaris);



- Symbian — программы ОС Symbian OS (мобильная ОС).

Заметим, что некоторые вредоносные программы могут заражать программы одной системы, хотя сами действуют в другой.

Вирусы, поражающие файлы MS Office

Группа префиксов вирусов, поражающих объекты MS Office (указан язык макросов, поражаемых данным типом вирусов):

- WM — Word Basic (MS Word 6.0-7.0);
- XM — VBA3 (MS Excel 5.0-7.0);
- W97M — VBA5 (MS Word 8.0), VBA6 (MS Word 9.0);
- X97M — VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0);
- A97M — базы данных MS Access'97/2000;
- PP97M — файлы-презентации MS PowerPoint;
- O97M — VBA5 (MS Office'97), VBA6 (MS Office'2000), вирус заражает файлы более чем одного компонента MS Office.

Префиксы языка разработки

Группа префиксов HLL применяется для именования угроз, написанных на языках программирования высокого уровня, таких как C, C++, Pascal, Basic и другие.

Используются модификаторы, указывающие на базовый алгоритм функционирования, в частности:

- HLLW — черви;
- HLLM — почтовые черви;
- HLLQ — вредоносные программы, перезаписывающие код программы жертвы;
- HLLP — паразитические вредоносные программы;
- HLLC — вредоносные программы-спутники.

К группе префиксов языка разработки можно также отнести:

- Java — угрозы для среды виртуальной машины Java.

Троянские программы

Trojan — общее название для различных Троянских программ (троянцев). Во многих случаях префиксы этой группы используются совместно с префиксом Trojan.

- PWS — троянец, ворующий пароли;
- Backdoor — троянец с RAT-функцией (Remote Administration Tool — утилита удаленного администрирования);



- IRC — троянец, использующий для своего функционирования среду Internet Relayed Chat channels;
- DownLoader — троянец, скрытно от пользователя загружающий различные вредоносные файлы из интернета;
- MulDrop — троянец, скрытно от пользователя загружающий различные вредоносные файлы, содержащиеся непосредственно в его теле;
- Proxy — троянец, позволяющий злоумышленнику работать в интернете анонимно через пораженный компьютер;
- StartPage (синоним: Seeker) — троянец, несанкционированно подменяющий адрес страницы, указанной браузеру в качестве домашней (стартовой);
- Click — троянец, организующий перенаправление пользовательских запросов браузеру на определенный сайт (или сайты);
- KeyLogger — троянец-шпион; отслеживает и записывает нажатия клавиш на клавиатуре; может периодически пересылать собранные данные злоумышленнику;
- AVKill — останавливает работу программ антивирусной защиты, сетевые экраны и т. п.; также может удалять эти программы с диска;
- KillFiles, KillDisk, DiskEraser — удаляют некоторое множество файлов (файлы в определенных каталогах, файлы по маске, все файлы на диске и т. п.);
- DelWin — удаляет необходимые для работы операционной системы (Windows) файлы;
- FormatC — форматирует диск C: (синоним: FormatAll — форматирует несколько или все диски);
- KillMBR — портит или стирает содержимое главного загрузочного сектора (MBR);
- KillCMOS — портит или стирает содержимое CMOS.

Средство использования уязвимостей

- Exploit — средство, использующее известные уязвимости некоторой операционной системы или приложения для внедрения в систему вредоносной программы или выполнения каких-либо несанкционированных действий.

Средства для сетевых атак

- Nuke — средства для сетевых атак на некоторые известные уязвимости операционных систем с целью вызвать аварийное завершение работы атакуемой системы;
- DDoS — программа-агент для проведения распределенных сетевых атак типа «отказ в обслуживании» (Distributed Denial Of Service);
- FDOS (синоним: Flooder) — Flooder Denial Of Service — программы для разного рода вредоносных действий в Сети, так или иначе использующие идею атаки типа «отказ в обслуживании»; в отличие от DDoS, где против одной цели одновременно используется множество агентов, работающих на разных компьютерах, FDOS-программа работает как отдельная, «самодостаточная» программа.



Скрипт-угрозы

Префиксы угроз, написанных на различных языках сценариев:

- `VBS` — Visual Basic Script;
- `JS` — Java Script;
- `Wscript` — Visual Basic Script и/или Java Script;
- `Perl` — Perl;
- `PHP` — PHP;
- `BAT` — язык командного интерпретатора ОС MS-DOS.

Вредоносные программы

Префиксы объектов, являющихся не вирусами, а иными вредоносными программами:

- `Adware` — рекламная программа;
- `Dialer` — программа дозвона (перенаправляющая звонок модема на заранее запрограммированный платный номер или платный ресурс);
- `Joke` — программа-шутка;
- `Program` — потенциально опасная программа (riskware);
- `Tool` — программа-инструмент взлома (hacktool).

Разное

Префикс `generic` используется после другого префикса, обозначающего среду или метод разработки, для обозначения типичного представителя этого типа угроз. Такая угроза не обладает никакими характерными признаками (как текстовые строки, специальные эффекты и т. д.), которые позволили бы присвоить ей какое-то особенное название.

Ранее для именования простейших безликих вирусов использовался префикс `Silly` с различными модификаторами.

Суффиксы

Суффиксы используются для именования некоторых специфических вредоносных объектов:

- `generator` — объект является не вирусом, а вирусным генератором;
- `based` — вредоносный объект разработан с помощью указанного генератора или путем видоизменения указанной угрозы. В обоих случаях имена этого типа являются родовыми и могут обозначать сотни и иногда даже тысячи угроз;



- `dropper` — указывает, что объект является не вирусом, а контейнером указанного вируса.



19. Приложение Г. Основные термины и понятия

А

Антивирусная сеть — совокупность компьютеров, на которых установлены продукты Dr.Web (Антивирус для Windows, Server Security Suite, Katana и Security Space) и которые подключены к одной локальной сети.

Архив — файл с упакованными в нем другими файлами и их метаданными. Возможные форматы: ARJ, GZIP, RAR, TAR, ZIP и т. п.

Д

Доверенные приложения — приложения, подписи которых добавлены в список доверенных в drwbase.db. К доверенным приложениям относится популярное ПО, такое как Google Chrome, Firefox, приложения Microsoft.

З

Зеркало обновлений — папка, в которую копируются обновления. Зеркало обновлений может быть использовано как источник обновлений Dr.Web для компьютеров в локальной сети, которые не подключены к интернету.

К

Классы устройств — устройства, выполняющие одинаковые функции (например, устройства для печати).

Контейнер — составной объект, который может быть распакован. Список форматов:

Проверяются всегда:

AUTOIT, BANGCLE, CHM, DOC1C, EMBEDOBJ, HTML, HTMLVBA, JAR, JSHTML, LNK, MSGVBA, ODEX, OLEEXPL, OPEN_XML, PDF, PPT, RC, RTF, SECSHELL, SWF, TENCENT, VISIO.

Проверяются при запуске:

NSIS, NSIS_as, PYINSTALL.

Проверяются при включенной опции **Проверять контейнеры**:

ADVINST, ASF, BCOMPILER, CLICKTEAM, CMTSCRIPT, CREATEINSTALL, DDS, DEB, DEPLOY, GKWARE, GTP, IJAMMER, INNO, ISHIELD, ISZ, JCOMPILER, LZMA, MACBIN, MSI, MSSE, MSXML, NETSTREAM, OCRA, PERL2EXE, PHP, PIMP, PYTHON, RPM, RSFX, SFACT, SFX74, SIM, SIS, SQUASH, TARMA, TCOMPR, THINST, UDF, UNIBIN, VISE, WIM, WISE, XAR, XENOCODE, XZ, ZLIB.



М

Модификация — код, полученный таким изменением известной угрозы, что при этом он опознается сканером, но алгоритмы лечения исходной угрозы к нему неприменимы.

П

Почтовый файл — файл почтового клиента, используемый для хранения различных данных электронной почты. Примеры форматов: DBX, MIME, PST, TBB, TNEF, UUE.

Р

Режим администратора — режим Dr.Web, в котором предоставляется доступ ко всем параметрам компонентов защиты и настройкам программы. Для перехода в режим администратора необходимо нажать на замок .

С

Сигнатура (запись об угрозе) — непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы.

Х

Хеш-сумма — уникальный идентификатор файла, представляющий собой последовательность цифр и букв заданной длины. Используется для проверки целостности данных.

Ш

Шины устройств — подсистемы передачи данных между функциональными блоками компьютера (например, шина USB).

Э

Эвристика — предположение, статистическая значимость которого подтверждена опытным путем.

Эксплойт — программа, фрагмент кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на систему.



Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Эмуляция — имитация работы одной системы средствами другой без потери функциональных возможностей и искажений результатов посредством использования специальных программных средств.

