Dr.WEB

FixIt!

Руководство пользователя

Dr.Web FixIt!
Версия 2.4
Руководство пользователя
16.01.2025

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. Условные обозначения 6
2. О продукте 7
3. Системные требования 9
4. Начало работы 11
   4.1. Авторизация 11
   4.2. Профиль 11
5. Учетные записи 13
   5.1. Администратор 17
   5.2. Менеджер 18
   5.3. Пользователь 19
6. Управление пространствами 20
   6.1. Как посмотреть список пространств 20
   6.2. Как создать пространство 20
   6.3. Как редактировать пространство 21
   6.4. Как заблокировать или разблокировать пространство 21
   6.5. Как искать пространства 22
   6.6. Как фильтровать пространства 22
7. Управление администраторами 24
8. Настройки Dr.Web 27
9. Фильтры 28
10. Пространство 31
11. Задачи 36
   11.1. Задача 38
   11.2. Журнал 42
   11.3. Экспертное сопровождение 45
12. Отчеты 48
   12.1. Как загрузить отчет в задачу 48
   12.2. Общая информация об отчете 49
   12.3. Сведения, собранные утилитой FixIt! 50
      12.3.1. Данные 50
      12.3.2. Система 72
      12.3.3. Файлы 74

12.4. Как посмотреть список отчетов 76
12.5. Как сравнить отчеты 77
12.6. Как скачать отчет 79
12.7. Как переименовать отчет 79
12.8. Как удалить отчет 79
13. Виджеты 80
13.1. Как анализировать отчет с помощью виджетов 80
13.2. Категории виджетов 81
13.3. Как посмотреть список виджетов 81
13.4. Как создать виджет 83
13.5. Как изменить виджет 84
13.6. Как включить или выключить виджет 84
13.7. Как удалить виджет 85
13.8. Как узнать состав виджета 86
13.9. Как управлять виджетами 87
14. Поиск и анализ 89
14.1. Готовые фильтры 89
14.2. Новый фильтр 92
14.2.1. Составление запросов 96
14.3. Выбранные действия 98
15. Утилита FixIt! 100
15.1. Как создать утилиту FixIt! 100
15.2. Настройки утилиты 101
15.3. Команды утилиты 102
15.3.1. Команды сбора информации 103
15.3.2. Команды лечения 106
15.4. Скрипт 115
15.5. Как проверить компьютер утилитой FixIt! 116
16. Техническая поддержка 118
17. Приложение А. Пример использования 119
18. Приложение Б. Список полей 127

1. 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.
Антивирусная сеть	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.
Приложение А	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.

2. О продукте

Dr.Web FixIt! — сервис для анализа безопасности компьютеров под управлением операционных систем семейства Microsoft Windows. Dr.Web FixIt! позволяет специалистам по информационной безопасности детально анализировать состояние компьютера, а также устранять выявленные вирусные угрозы и потенциальные уязвимости.

Работа с Dr.Web FixIt! осуществляется через веб-интерфейс, поэтому сервис не требует установки. Проанализировать файлы и устранить угрозы безопасности можно даже в том случае, если на проверяемых компьютерах установлены антивирусные продукты других производителей.

Гибкая настройка позволяет эффективно применять Dr.Web FixIt! в различных сценариях, таких как:

- анализ компьютера после известного случая заражения вредоносным ПО с последующим лечением;
- анализ компьютера при подозрении на вирусную активность;
- поиск следов вредоносной активности после заражения;
- поиск и анализ уязвимостей в компьютерной системе;
- устранение последствий заражения различным вредоносным ПО;
- сбор данных при расследовании целевых атак на информационные системы.

Для анализа и лечения устройства сервис генерирует специальную утилиту FixIt! с учетом выбранных параметров.

Подробную информацию о работе сервиса можно найти в **Справке о продукте**. Чтобы перейти к ней, нажмите значок  на верхней панели веб-интерфейса справа.

Как работает Dr.Web FixIt!

1. Вы создаете задачу в сервисе и отправляете владельцу проверяемого компьютера анализирующую утилиту FixIt!.
2. Владелец проверяемого компьютера запускает утилиту FixIt!. Утилита проверяет компьютер и формирует отчет о его состоянии.
3. Вы анализируете отчет в сервисе, создаете лечащую утилиту FixIt! и отправляете владельцу проверяемого компьютера.
4. Владелец проверяемого компьютера запускает утилиту FixIt!. Утилита выполняет заданный вами скрипт и формирует новый отчет.
5. Вы повторяете шаги 3 и 4 до тех пор, пока все угрозы на проверяемом компьютере не будут нейтрализованы, после чего закрываете задачу.

Задачи организованы в пространства — группы пользователей и менеджеров, объединенных принадлежностью к какой-либо категории (например, организации или отделу). Пользователи могут создавать свои задачи и просматривать другие задачи внутри своего пространства.

Менеджеры пространства управляют учетными записями пользователей.

Организацию работы с пространствами в сервисе осуществляют администраторы. Администраторам доступны все задачи, пространства и учетные записи сервиса.

3. Системные требования

Для корректной работы с сервисом Dr.Web FixIt! компьютер должен соответствовать следующим системным требованиям:

Параметр	Требования
Браузер	Один из: • Google Chrome 56.0 или более поздняя версия; • Mozilla Firefox 45.0 или более поздняя версия; • Safari 11.0 или более поздняя версия; • Microsoft Edge 44.0 и более поздняя версия; • любая версия Microsoft Edge Chromium
Разрешение экрана	Не менее 1024x768 пикселей

Для корректной работы утилиты FixIt! компьютер должен соответствовать следующим системным требованиям:

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 Server 2003 с пакетом обновлений SP1; • Windows Server 2008 с пакетом обновлений SP2 или более поздними; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10. Для 64-разрядных операционных систем: • Windows Server 2008 с пакетом обновлений SP2 или более поздними; • Windows Server 2008 R2 с пакетом обновлений SP1 или более поздними; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019; • Windows Server 2022; • Windows Vista; • Windows 7;

Параметр	Требования
	• Windows 8; • Windows 8.1; • Windows 10; • Windows 11
Место на жестком диске	Не менее 1 ГБ
Оперативная память	256 МБ и больше

4. Начало работы

Для начала работы с Dr.Web FixIt! необходимо приобрести лицензию и авторизоваться в сервисе FixIt!.

Приобрести лицензию Dr.Web FixIt! можно на сайте компании «Доктор Веб».

4.1. Авторизация

В качестве параметров авторизации используются логин и пароль. Получите данные авторизации от лица, зарегистрировавшего вас в сервисе.

Чтобы авторизоваться в сервисе

1. Откройте страницу входа в Dr.Web FixIt!.
2. Введите полученные логин и пароль.
3. Установите флажок **Запомнить меня**, если вы хотите сохранить параметры авторизации.
4. Нажмите **Войти**.

> Если вы не будете совершать никаких действий в сервисе в течение 1 часа (при этом флажок **Запомнить меня** на главной странице сервиса не установлен), сеанс автоматически завершится с переходом на главную страницу, а внизу страницы отобразится предупреждение.

4.2. Профиль

В правом верхнем углу веб-интерфейса Dr.Web FixIt! расположено меню **Профиль**.

В меню **Профиль** доступны следующие опции:

- **Настройки:** позволяет выбрать язык интерфейса и сменить текущий пароль, если эта возможность предусмотрена для учетной записи.
- **Выйти:** позволяет выйти из системы.

Чтобы сменить язык интерфейса

1. В выпадающем списке **Язык** выберите нужный язык интерфейса.
2. Нажмите **Сохранить**.

Чтобы изменить пароль

3. Введите текущий пароль, а затем дважды новый.
4. Нажмите **Сохранить**.

Возможность смены пароля зависит от типа учетной записи: для учетной записи пользователя она может отсутствовать.

5. Учетные записи

В Dr.Web FixIt! есть три типа учетных записей (роли): администратор, менеджер и пользователь. Возможность использования некоторых функций Dr.Web FixIt! зависит от типа учетной записи.

В таблице ниже показано, какие действия доступны пользователям в зависимости от их роли.

Действия	Администратор	Менеджер	Пользователь	Примечания
Пространства				
Создавать пространства	да	нет	нет	
Редактировать пространства	да	нет	нет	
Блокировать и открывать пространства	да	нет	нет	
Устанавливать лимит задач для пространства	да	нет	нет	
Задавать время жизни задач для пространства	да	нет	нет	
Добавлять связанные пространства	да	нет	нет	
Просматривать список связанных пространств	да	нет	нет	Менеджеры и пользователи не могут посмотреть список связанных пространств, но могут поделиться задачей с пространством из этого списка.
Учетные записи				
Создавать учетные записи	да	да	нет	Администратор может создавать других

Действия	Администратор	Менеджер	Пользователь	Примечания
				администраторов, а также менеджеров и пользователей пространств. Менеджер может удалять только менеджеров и пользователей внутри своего пространства.
Удалять учетные записи	да	да	нет	Администратор может удалять других администраторов, а также менеджеров и пользователей пространств. Менеджер может удалять только менеджеров и пользователей внутри своего пространства.
Изменять тип учетной записи	да	да	нет	
Изменять пароль учетной записи	да	да	нет	Администратор может изменять пароли других администраторов, а также менеджеров и пользователей пространств. Менеджер может изменять пароли только менеджеров и пользователей внутри своего пространства.
Блокировать и повторно	да	да	нет	Администратор может

Действия	Администратор	Менеджер	Пользователь	Примечания
активировать учетную запись				блокировать и повторно активировать других администраторов, а также менеджеров и пользователей пространств. Менеджер может изменять блокировать и повторно активировать только менеджеров и пользователей внутри своего пространства.
Задачи				
Создавать задачи	да	да	да	
Переименовывать задачи	да	да	да	
Закрывать задачи	да	да	да	
Переоткрывать задачи	да	да	да	
Удалять задачи	да	да	нет	
Делиться задачами со связанными пространствами	да	да	да	
Запрашивать экспертное сопровождение задач	да	да	да	
Фильтры				
Создавать фильтры	да	да	да	Администраторы могут создавать фильтры **Для**

Действия	Администратор	Менеджер	Пользователь	Примечания
				всех, **Для задачи** и **Для меня**. Менеджеры и пользователи могут создавать фильтры **Для пространства**, **Для задачи** и **Для меня**. Фильтры **Для пространства** видны только менеджерам и пользователям этого пространства. Фильтры **Для меня** видны только автору фильтра (это может быть администратор, менеджер или пользователь).
Изменять доступность фильтров	да	да	да	Менеджеры и пользователи не могут изменять фильтры **Для всех**.
Изменять фильтры	да	да	да	Менеджеры и пользователи не могут изменять фильтры **Для всех**.
Добавлять фильтры в группы	да	да	да	Менеджеры и пользователи не могут изменять фильтры **Для всех**.
Удалять фильтры	да	да	да	Менеджеры и пользователи не могут удалять фильтры **Для всех**.

Действия	Администратор	Менеджер	Пользователь	Примечания
Отчеты				
Переименовывать отчеты	да	да	да	
Удалять отчеты	да	да	нет	
Виджеты				
Создавать виджеты	да	да	да	Администраторы могут создавать виджеты **Для всех**, **Для задачи** и **Для меня**. Менеджеры и пользователи могут создавать виджеты **Для пространства**, **Для задачи** и **Для меня**.
Включать и выключать виджеты	да	да	да	
Изменять виджеты	да	да	да	
Удалять виджеты	да	да	да	

5.1. Администратор

Администратор имеет доступ ко всем пространствам, задачам и учетным записям сервиса. Администратор может:

- управлять пространствами:
  - создавать новые пространства;
  - редактировать пространства;
  - блокировать и разблокировать пространства;
  - устанавливать лимит на создание задач в пространстве;
  - задавать срок действия задач в пространстве;
  - добавлять связанные пространства, с которыми можно делиться задачами;
  - просматривать списки пространств, связанных с другими пространствами;
- управлять учетными записями:

    - создавать администраторов;
    - создавать менеджеров и пользователей внутри пространств;
    - удалять учетные записи администраторов, менеджеров и пользователей;
    - менять тип учетной записи внутри пространства;
    - сбрасывать пароли к учетным записям администраторов, менеджеров и пользователей;
    - блокировать и активировать учетные записи администраторов, менеджеров и пользователей;
- вносить изменения в список задач:
    - переоткрывать задачи;
    - переименовывать задачи;
    - закрывать задачи;
    - удалять задачи;
    - делиться задачами;
    - запрашивать экспертное сопровождение задач;
- редактировать фильтры:
    - создавать новые фильтры;
    - менять доступность любых фильтров;
    - добавлять любые фильтры в группы;
    - удалять любые фильтры;
- переименовывать и удалять отчеты.

5.2. Менеджер

Менеджер имеет доступ ко всем задачам и учетным записям пространства, к которому он принадлежит. Он может:

- управлять учетными записями внутри своего пространства:
    - создавать менеджеров и пользователей внутри пространства;
    - удалять учетную запись;
    - изменять имя или электронную почту учетной записи;
    - менять тип учетной записи внутри пространства;
    - сбрасывать пароль к учетной записи;
    - блокировать и активировать учетную запись внутри пространства;
- вносить изменения в список задач в своем пространстве:
    - переоткрывать задачи;
    - переименовывать задачи;
    - закрывать задачи;

    - удалять задачи;
    - делиться задачами со связанными пространствами из списка, составленного администратором;
    - запрашивать экспертное сопровождение задач;
- редактировать фильтры пространства:
    - создавать новые фильтры;
    - удалять фильтры;
    - изменять фильтры;
    - добавлять фильтры в группы.

5.3. Пользователь

Пользователь имеет доступ ко всем задачам своего пространства. Он может:

- менять пароль своей учетной записи;
- вносить изменения в свой список задач:
    - создавать задачи;
    - переименовывать задачи;
    - закрывать задачи;
    - делиться задачами со связанными пространствами из списка, составленного администратором;
    - запрашивать экспертное сопровождение задач;
- редактировать фильтры пространства:
    - добавлять фильтры;
    - удалять фильтры;
    - изменять фильтры;
    - добавлять фильтры в группы.

6. Управление пространствами

У администратора есть доступ ко всем пространствам сервиса. Он может:

- Просматривать список всех пространств
- Создавать пространства
- Редактировать пространства
- Блокировать и разблокировать пространства
- Добавлять связанные пространства

6.1. Как посмотреть список пространств

Сводная таблица всех пространств сервиса содержится на вкладке **Пространства** страницы **Управление**.

Чтобы открыть эту вкладку, на верхней панели FixIt! выберите **Управление**.

Для каждого пространства в таблице приведена следующая информация:

- **Пространство:** имя пространства.
- **Статус:** Активно или Заблокировано.
- **Лимит задач:** количество задач, использованных в данном пространстве. Если лимит для пространства не задан, в этом столбце будет указано значение **Безлимитно**.
- **Участники:** общее количество менеджеров и пользователей пространства.
- **Последнее изменение:** дата и время последнего изменения, внесенного в пространство.

Вы можете отсортировать строки в таблице пространств по содержимому любого столбца. Для этого нажмите заголовок этого столбца. Чтобы изменить порядок сортировки на противоположный, нажмите заголовок еще раз.

Чтобы перейти на страницу с подробной информацией о пространстве, нажмите его имя в таблице пространств.

6.2. Как создать пространство

Администраторы могут создавать пространства и добавлять в них участников (менеджеров и пользователей).

Чтобы создать пространство

1. Нажмите кнопку  над таблицей.

2. В окне **Новое пространство** в поле **Имя** укажите имя нового пространства.
3. При необходимости вы можете установить лимит на количество задач в пространстве и срок действия задач. Для этого установите флажки и укажите в полях рядом нужные значения.
4. Нажмите **Сохранить**.

6.3. Как редактировать пространство

Вы можете изменить имя пространства, лимит задач и срок их действия, а также состав участников.

Чтобы изменить имя пространства, лимит задач и срок их действия

1. В правой части строки пространства нажмите  .
2. Внесите необходимые изменения.
3. Нажмите **Сохранить**.

Чтобы изменить состав участников

1. Нажмите имя пространства в таблице пространств.
2. Создайте участника или удалите существующего.

6.4. Как заблокировать или разблокировать пространство

Как заблокировать пространство

Если сотрудничество с участниками пространства по той или иной причине завершено, пространство можно заблокировать. В этом случае менеджеры и пользователи не смогут продолжить работу в нем. При входе в FixIt! они увидят предупреждение, что их пространство заблокировано.

Чтобы заблокировать пространство

- Через сводную таблицу пространств
  1. В правой части строки пространства нажмите  .
  2. Нажмите **Заблокировать**.
- На странице самого пространства
  1. В таблице пространств нажмите имя пространства.
  2. В правом верхнем углу страницы пространства выберите ··· > **Заблокировать пространство**.

3. Нажмите **Заблокировать**.

Как разблокировать пространство

Вы можете повторно открыть ранее заблокированное пространство.

Чтобы разблокировать пространство

- Через сводную таблицу пространств: в правой части строки пространства нажмите  .
- На странице самого пространства
  1. В таблице пространств нажмите имя пространства.
  2. В правом верхнем углу страницы пространства выберите ··· > **Разблокировать пространство**.

6.5. Как искать пространства

Вы можете выполнять поиск по содержимому сводной таблицы пространств. Для удобства и скорости поиск будет выполняться по мере ввода символов в строке поиска.

Чтобы выполнить поиск пространства

1. Введите запрос в поле  **Поиск** над таблицей.
2. Чтобы зафиксировать запрос, нажмите левую кнопку мыши вне поля поиска или клавишу ENTER.

Поиск и фильтрация выполняются по данным, отображающимся в таблице. Таким образом, если вы задали фильтр или выполнили поисковый запрос по таблице, последующая операция фильтрации или поиска будет применена к результатам предыдущей.

6.6. Как фильтровать пространства

Для удобства просмотра вы можете фильтровать содержимое таблицы пространств по имени пространства, статусу и дате последнего изменения.

Чтобы задать фильтр для таблицы пространств

1. Нажмите  над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Имя** или **Статус**:

- Установите флажки напротив нужных вам значений и нажмите **Добавить**.

Если вы выбрали параметр **Последнее изменение**:

- Нажмите нужную вам дату. Чтобы задать период времени, нажмите дату начала периода и потяните курсор до даты окончания периода. Затем нажмите **Применить**.

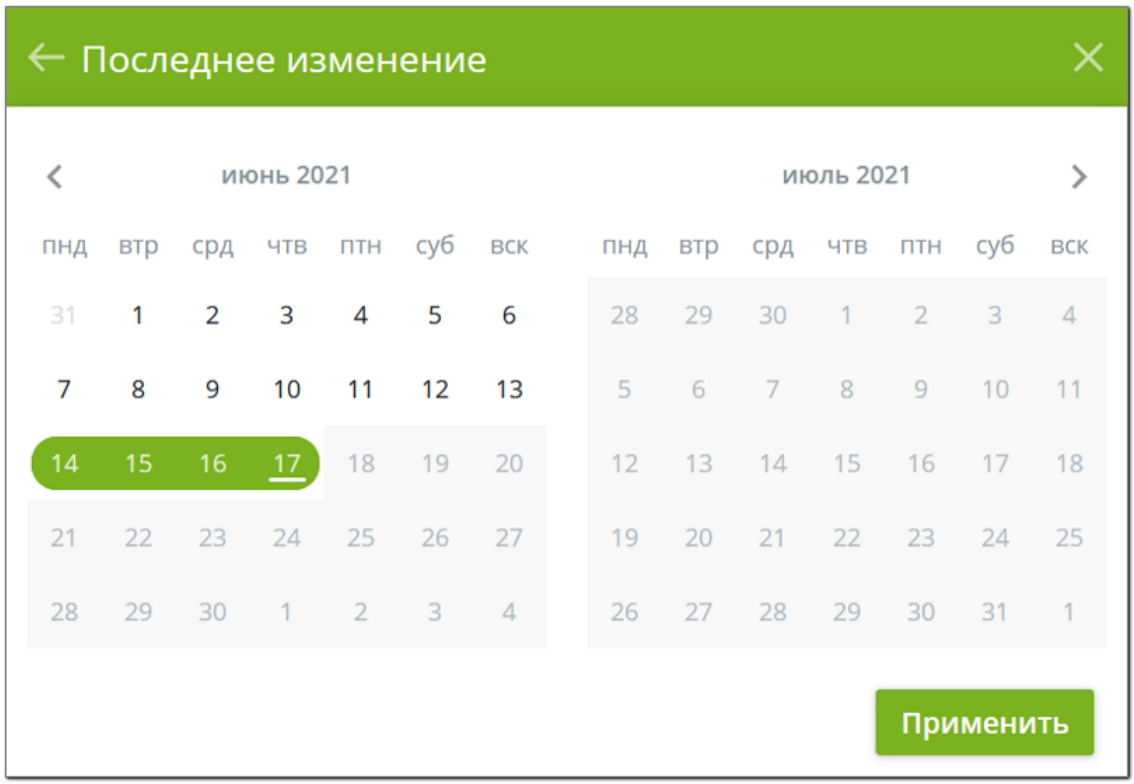

Рисунок 1. Фильтрация по периоду

В окне **Фильтр** за раз можно выбрать только один параметр. Если вам нужно отфильтровать пространства по нескольким параметрам, задайте последовательно несколько фильтров.

Поиск и фильтрация выполняются по данным, отображающимся в таблице. Таким образом, если вы задали фильтр или выполнили поисковый запрос по таблице, последующая операция фильтрации или поиска будет применена к результатам предыдущей.

7. Управление администраторами

На вкладке **Администраторы** содержится сводная таблица всех администраторов сервиса. Для каждого администратора в таблице указывается следующая информация:

- **Имя**.
- **Электронная почта**.
- **Статус**: Активен или Заблокирован.
- **Задачи (Открыто/Закрыто)**: количество задач, открытых и закрытых администратором.
- **Дата создания**.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы.

Фильтрация и поиск

Для удобства просмотра данных администраторов сервиса вы можете фильтровать содержимое сводной таблицы администраторов и выполнять поиск по содержимому таблицы.

Таблицу можно фильтровать по следующим параметрам учетной записи администратора:

- имя,
- электронная почта,
- статус,
- дата создания.

Чтобы задать фильтр для таблицы администраторов

1. Нажмите над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Имя**, **Электронная почта** или **Статус**:
   - Установите флажки напротив интересующих вас значений и нажмите **Добавить**.

   Если вы выбрали параметр **Дата создания**:
   - Нажмите интересующие вас даты. Чтобы задать период времени, нажмите дату начала периода и потяните курсор до даты окончания периода. Затем нажмите **Применить**.

Для фильтра можно выбрать только один параметр. Задайте несколько фильтров, чтобы отфильтровать таблицу администраторов по нескольким параметрам одновременно.

Чтобы выполнить поиск по таблице администраторов

1. Введите запрос в поле **Поиск** над таблицей. Поиск выполняется динамически в процессе набора.
2. Нажмите левую кнопку мыши вне поля поиска или клавишу ENTER, чтобы зафиксировать запрос.

Поиск и фильтрация выполняются по данным таблицы в текущем виде. Если вы задали фильтр или выполнили поисковый запрос по таблице, последующая операция фильтрации или поиска будет применена к результатам предыдущей.

Управление учетными записями администраторов

На вкладке **Администраторы** также можно управлять учетными записями администраторов: создать новую учетную запись; редактировать или удалить существующую.

Чтобы создать учетную запись администратора

1. Нажмите **Управление** в правом верхнем углу страницы.
2. Перейдите на вкладку **Администраторы**.
3. Нажмите кнопку .
4. В окне **Новый администратор** укажите данные администратора: имя, адрес электронной почты и пароль.
5. Нажмите кнопку **Создать**.

Вы можете редактировать параметры учетной записи администратора: имя, адрес электронной почты и статус. Вы также можете задать новый пароль учетной записи администратора.

Чтобы редактировать учетную запись администратора

1. В правой части строки учетной записи, которую вы хотите отредактировать, нажмите .
2. В окне **Информация об администраторе** внесите необходимые изменения.
3. Нажмите **Сохранить**.

В окне редактирования учетной записи администратора возможно заблокировать администратора. Администратор не сможет продолжить работу в системе после блокировки. Разблокировать учетную запись администратора может только администратор.

Чтобы заблокировать или разблокировать учетную запись администратора, воспользуйтесь переключателем **Статус** в окне редактирования.

Вы также можете удалить учетную запись администратора, если его работа в сервисе завершена. Восстановить учетную запись после удаления будет невозможно.

Чтобы удалить учетную запись администратора

1. В правой части строки учетной записи, которую вы хотите удалить, нажмите  .
2. Нажмите **Удалить**.

Удаление администратора не приведет к удалению созданных им пространств и задач.

8. Настройки Dr.Web

Вкладка **Настройки Dr.Web** находится на верхней панели сервиса. Этот раздел позволяет добавлять, просматривать и изменять стандартные (по умолчанию) настройки продукта компании «Доктор Веб», установленного на компьютере. Раздел доступен только администраторам.

Информация в этом разделе представлена в виде таблицы со следующими графами:

- **Настройка** — заданное администратором название настройки продукта;
- **Версия** — версия продукта;
- **Ключ** — ключ этой настройки в реестре Windows;
- **Параметр** — параметр в реестре Windows;
- **Значение** — значение параметра в реестре Windows;
- **Описание** — информация о настройке.

Администратор добавляет настройки вручную, указывая для них всю необходимую информацию.

Чтобы добавить настройку

1. Нажмите вверху страницы.
2. В окне **Добавление настройки** введите сведения о настройке.
3. Нажмите **Сохранить**.

Кнопка **Сохранить** станет доступна, когда вы заполните все обязательные поля. Обязательными являются все поля, кроме поля **Описание**.

Чтобы изменить настройку

1. В правой части строки настройки, которую вы хотите изменить, нажмите .
2. В окне **Изменение настройки** введите новые сведения.
3. Нажмите **Сохранить**.

Чтобы удалить настройку

1. В правой части строки настройки, которую вы хотите удалить, нажмите .
2. В окне **Удаление настройки** нажмите **Удалить**.

9. Фильтры

Вкладка **Фильтры** находится на верхней панели сервиса. Этот раздел позволяет создавать и изменять фильтры, которые используются для поиска данных в отчете (см. раздел Поиск и анализ). Фильтры облегчают анализ данных отчета, поскольку выводят только ту информацию, которая вас интересует. Раздел **Фильтры** служит для того, чтобы просматривать, создавать и редактировать фильтры и группы фильтров, не выполняя при этом анализ данных конкретного отчета.

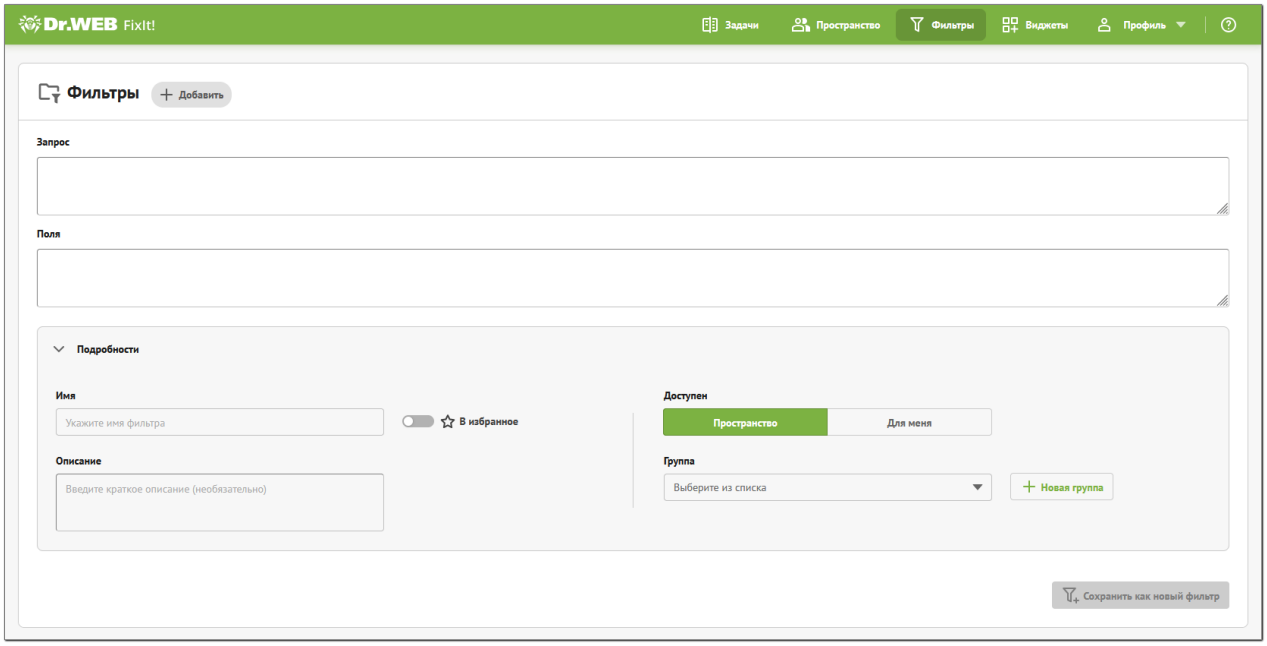

Рисунок 2. Фильтры

Администратор может создавать, редактировать и удалять любые фильтры, включая предустановленные. Менеджер и пользователь могут создавать, редактировать и удалять фильтры, созданные в пространстве, к которому принадлежит менеджер или пользователь.

Фильтр состоит из следующих компонентов:

- **Запрос** — по нему выполняется поиск по данным. Запрос состоит из аргументов (категорий объектов, по которым выполняется поиск) и их значений (то есть параметров конкретных объектов внутри категории).
- **Поле** — определяет то, какие поля будут выведены в результате запроса. В одном фильтре может быть несколько полей, которые указываются через запятую.

Более подробная информация о запросах и полях приведена в разделе Составление запросов.

Вы можете настроить доступ к фильтру, сделав его видимым для других пользователей сервиса или только для вас. Возможны следующие варианты доступа:

- **Для всех** — опция доступна только для администраторов. Фильтр будет виден всем участникам сервиса.
- **Для этого пространства** — опция доступна только для менеджеров и пользователей. Фильтр будет виден всем участникам пространства.
- **Для меня** — опция доступна всем участникам сервиса. Фильтр будет виден только участнику, создавшему фильтр.

Чтобы создать фильтр

1. Заполните поля **Запрос** и **Поля**.
2. На панели **Подробности** заполните поля **Имя** и **Описание**.
3. При желании добавьте фильтр в избранное, установив переключатель **В избранное**.
4. В поле **Доступен** укажите, кому будет доступен фильтр.
5. Выберите группу или создайте новую, нажав **Новая группа**.
6. Нажмите **Сохранить как новый фильтр**.

> Администраторы могут скрыть указанные в поле **Запрос** данные, используя переключатель **Скрыть запрос**.

Чтобы редактировать фильтр

1. В верхней части вкладки **Фильтры** нажмите **Добавить** и выберите фильтр, который хотите изменить.
2. Внесите изменения в соответствующие поля (см. Рисунок 3).
3. При необходимости измените доступность фильтра в поле **Доступен**.
4. Выберите группу или создайте новую, нажав **Новая группа**.

5. Нажмите **Сохранить изменения**, чтобы применить изменения. Чтобы создать новый фильтр, нажмите **Сохранить как новый фильтр**.

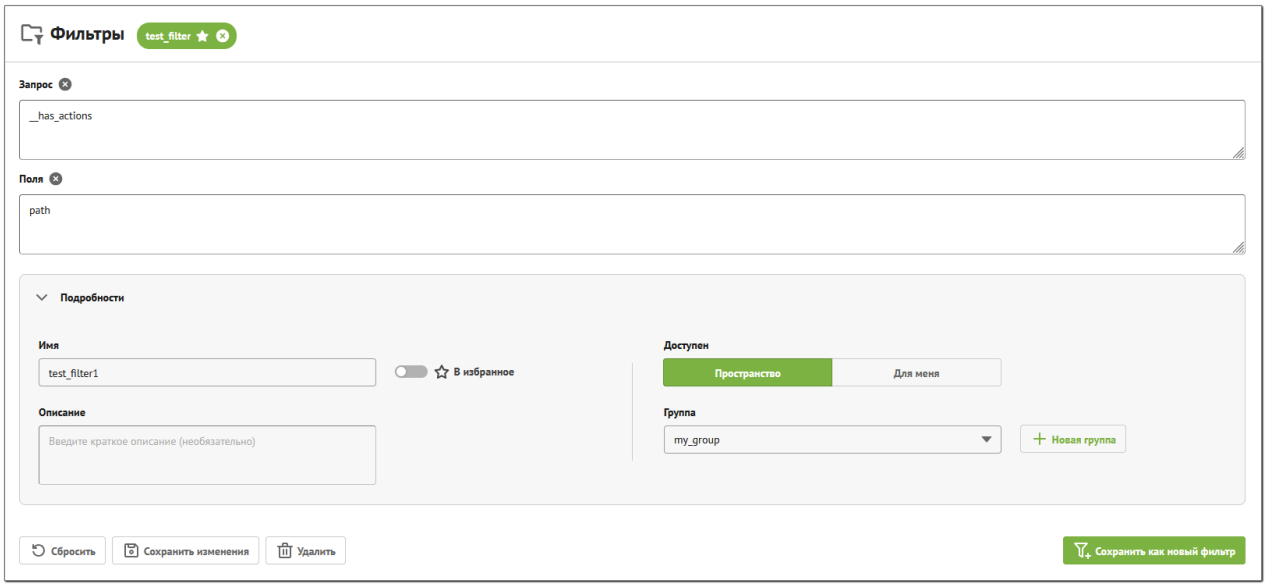

Рисунок 3. Редактирование фильтра

Чтобы удалить фильтр

1. В верхней части вкладки **Фильтры** нажмите **Добавить** и выберите фильтр, который хотите удалить.
2. Нажмите **Удалить.**
3. Во всплывающем окне **Удалить фильтр** подтвердите удаление.

В случае успешного создания, редактирования или удаления фильтра в левом нижнем углу экрана появится соответствующее уведомление. Вы можете отменить удаление фильтра, нажав кнопку **Отменить** на уведомлении.

Группы фильтров

Для удобства созданные фильтры можно объединять в группы. Если при создании фильтра вы не указали группу, фильтр по умолчанию сохранится в **No group**. Новая группа может быть создана только при редактировании фильтра на вкладке **Фильтры** или при создании фильтра на вкладке **Фильтры** или **Поиск и анализ**.

10. Пространство

Пространство — это группа менеджеров и пользователей.

Внутри пространства менеджеры могут управлять задачами и учетными записями пользователей и других менеджеров. Пользователи внутри пространства могут создавать задачи, работать с ними, а также просматривать задачи других пользователей пространства. Менеджерам и пользователям доступно только свое пространство. Новое пространство может создать только администратор.

Пространства могут быть связаны с другими пространствами. В таком случае менеджеры и пользователи могут делиться задачами своего пространства со связанными пространствами и получать доступ к задачам связанных пространств, которыми с ними поделятся. Добавлять связанные пространства могут только администраторы.

Страница пространства на вкладке **Пространство** в верхней части экрана доступна менеджерам и пользователям. Администратор может перейти на страницу пространства из раздела Пространства.

Вкладка Пространство

На вкладке **Пространство** содержится подробная информация о пространстве, а также сводная таблица участников пространства.

Для пространства доступна следующая информация:

- **Имя пространства**: отображается в верхней части страницы.
- **Срок действия задач**: срок, в течение которого над задачами этого пространства можно производить новые действия. По умолчанию он составляет 10 дней. По истечении этого срока доступными останутся только уже готовые отчеты.
- **Использовано задач**: количество задач, созданных в текущем пространстве, по сравнению с установленным лимитом. Если лимит не установлен, отображается значение Безлимитно.
- **Участники**: общее количество менеджеров и пользователей пространства.
- **Дата создания**: дата и время создания пространства.
- **Заметка**: описание пространства.

Описание пространства может добавить или редактировать только администратор или менеджер пространства. Нажмите + Заметка, чтобы добавить описание. Чтобы изменить или удалить описание, нажмите ⋮ справа от описания пространства и выберите соответствующую опцию.

Изменять имя пространства, лимит задач и срок их действия, а также блокировать пространство могут только администраторы.

Участники пространства

Снизу от информации о пространстве располагается сводная таблица всех участников пространства. Для каждого участника в таблице доступна следующая информация:

- **Имя**.
- **Электронная почта**.
- **Роль**: Менеджер или Пользователь.
- **Статус**: Активен или Заблокирован.
- **Задачи (Открыто/Закрыто)**: количество задач, открытых и закрытых участником.
- **Дата создания**.

Данные таблицы можно упорядочить, нажав значок  в нужном столбце таблицы.

Фильтрация и поиск

Для удобства просмотра данных участников пространства вы можете фильтровать содержимое сводной таблицы участников и выполнять поиск по содержимому таблицы.

Таблицу можно фильтровать по следующим параметрам учетной записи участника:

- имя,
- электронная почта,
- статус,
- дата создания.

Чтобы задать фильтр для таблицы участников

1. Нажмите  над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Имя**, **Электронная почта** или **Статус**:
   - Установите флажки напротив интересующих вас значений и нажмите **Добавить**.

   Если вы выбрали параметр **Дата создания**:
   - Нажмите интересующие вас даты. Чтобы задать период времени, нажмите дату начала периода и потяните курсор до даты окончания периода. Затем нажмите **Применить**.

Для фильтра можно выбрать только один параметр. Задайте несколько фильтров, чтобы отфильтровать таблицу участников пространства по нескольким параметрам одновременно.

Чтобы выполнить поиск по таблице участников

1. Введите запрос в поле **Поиск** над таблицей. Поиск выполняется динамически в процессе набора.
2. Нажмите левую кнопку мыши вне поля поиска или клавишу ENTER, чтобы зафиксировать запрос.

Поиск и фильтрация выполняются по данным таблицы в текущем виде. Если вы задали фильтр или выполнили поисковый запрос по таблице, последующая операция фильтрации или поиска будет применена к результатам предыдущей.

Управление учетными записями участников

На вкладке **Пространство** администраторы и менеджеры также могут управлять учетными записями участников: создать новую учетную запись, редактировать или удалить существующую. Пользователи могут редактировать данные только своей учетной записи в меню Профиль.

Чтобы создать учетную запись участника

1. Нажмите кнопку над сводной таблицей участников пространства.
2. В окне **Новый пользователь** укажите данные участника: роль (**Менеджер** или **Пользователь**), имя, адрес электронной почты и пароль.
3. Нажмите **Сохранить**.

При необходимости администратор или менеджер может редактировать данные учетной записи участника: изменить роль участника в пространстве (Менеджер или Пользователь), имя, электронную почту, заблокировать или разблокировать участника, а также задать новый пароль от его учетной записи.

Чтобы редактировать учетную запись участника

1. В правой части строки учетной записи, которую вы хотите изменить, нажмите .
2. Во всплывающем окне **Информация о пользователе** внесите необходимые изменения.
3. Нажмите **Сохранить**.

В окне редактирования учетной записи участника пространства можно заблокировать участника. Участник не сможет продолжить работу в системе после блокировки. Разблокировать учетную запись участника может только администратор или менеджер.

Чтобы заблокировать или разблокировать учетную запись участника, воспользуйтесь переключателем **Статус** в окне редактирования.

Вы также можете удалить учетную запись участника, если его работа в сервисе завершена. Восстановить учетную запись после удаления будет невозможно.

Чтобы удалить учетную запись участника

1. В правой части строки учетной записи, которую вы хотите удалить, нажмите .
2. Нажмите **Удалить**.

Связанные пространства

Dr.Web FixIt! позволяет создавать двусторонние связи между пространствами, благодаря которым можно открывать доступ к задачам участникам других пространств. Это может быть актуально при наличии нескольких пространств, принадлежащих одной организации.

Связи между пространствами может создавать только администратор. Менеджеры и пользователи могут делиться задачами со связанными пространствами.

Список связанных пространств с возможностью редактирования доступен администратору по нажатию кнопки **Связанные пространства** на странице пространства.

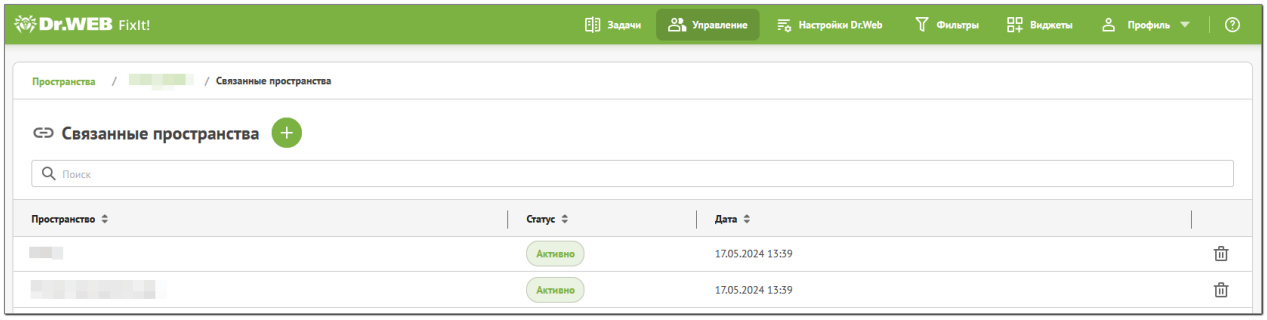

Рисунок 4. Связанные пространства

Чтобы добавить связанное пространство

1. Нажмите рядом с заголовком страницы.
2. В окне **Добавить пространство** выберите одно или несколько пространств, с которыми вы хотите установить связь.
3. Нажмите **Добавить**.

После этого менеджеры и пользователи обоих пространств смогут открывать друг другу доступ к задачам своих пространств.

Список запросов на сопровождение

Со страницы пространства можно перейти к списку запросов на экспертное сопровождение для всех задач этого пространства.

Чтобы перейти на страницу **Запросы на сопровождение**, нажмите кнопку **Запросы на сопровождение** в правом верхнем углу страницы.

11. Задачи

Задачи служат для организации работы по отслеживанию состояния проверяемых компьютеров. В рамках задачи можно создать анализирующую утилиту FixIt! с необходимыми параметрами, получить отчет о состоянии системы, проанализировать полученные данные и создать утилиту FixIt! для дальнейшего анализа и лечения системы. Для каждого компьютера создается отдельная задача.

Администраторы могут просматривать все задачи сервиса. Менеджерам и пользователям доступны только задачи пространства, к которому принадлежит менеджер или пользователь. Любой участник пространства может продолжить работу в открытой задаче, созданной другим участником пространства.

Задачи имеют *срок действия*, по истечении которого все сформированные отчеты останутся доступны, но новые действия с задачей больше нельзя будет производить. Этот параметр задается при создании пространства и применяется к каждой задаче в рамках пространства. По умолчанию срок действия составляет 10 дней.

Информация о задачах

На главной странице сервиса вы можете ознакомиться с информацией о задачах, а также перейти к работе над конкретной задачей. Чтобы перейти на главную страницу сервиса, нажмите **Задачи** на верхней панели FixIt! или логотип Dr.Web FixIt! в левом верхнем углу экрана.

В верхней части главной страницы содержится общая информация о задачах сервиса (для администратора) или пространства (для менеджера и пользователя). В зависимости от роли участника доступны следующие данные:

- **Использовано задач:** количество уже использованных задач из установленного лимита, если лимит задан (для менеджера или пользователя).
- **Открыто:** количество открытых задач сервиса (для администратора) или пространства (для менеджера или пользователя).
- **Закрыто:** количество закрытых задач сервиса (для администратора) или пространства (для менеджера или пользователя).

Таблица Задачи

Снизу от информации о задачах расположена сводная таблица задач.

Для каждой задачи в таблице доступна следующая информация:

- **Имя задачи**.
- **Срок действия**.
- **Создатель**.

- **Статус:** Открыто или Закрыто.
- **Пространство** (доступно только для администраторов).
- **Отчеты:** количество отчетов, полученных в рамках задачи.
- **Источник** (доступно только для менеджеров и пользователей).
- **Дата создания**.
- **Последнее изменение**.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы.

Чтобы начать или продолжить работу в сервисе, создайте новую или выберите существующую задачу.

Чтобы создать новую задачу

1. Нажмите кнопку справа от заголовка **Задачи**.
2. Введите имя новой задачи.
3. Нажмите **Создать задачу**.

Чтобы перейти к задаче

- Нажмите имя задачи в сводной таблице задач.

Фильтрация и поиск

Для удобства навигации таблицу задач можно фильтровать по следующим параметрам задачи:

- **Создатель**.
- **Пространство** (если доступно).
- **Статус**.
- **Дата создания**.
- **Последнее изменение**.

Чтобы задать фильтр для таблицы задач

1. Нажмите над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Создатель**, **Пространство** или **Статус**:
   - Установите флажки напротив интересующих вас значений и нажмите **Добавить**.

   Если вы выбрали параметр **Дата создания** или **Последнее изменение**:

- Нажмите интересующие вас даты. Чтобы задать период времени, нажмите дату начала периода и потяните курсор до даты окончания периода. Затем нажмите **Применить**.

Для каждого фильтра можно выбрать только один параметр. Чтобы отфильтровать таблицу задач одновременно по нескольким параметрам, задайте несколько фильтров.

Чтобы выполнить поиск по таблице задач

1. Введите запрос в поле  **Поиск** над таблицей. Поиск выполняется динамически в процессе набора.
2. Чтобы закончить ввод запроса, нажмите левую кнопку мыши вне поля поиска или клавишу ENTER.

Поиск и фильтрация выполняются по текущим данным, отображаемым в таблице. Если вы применили к таблице фильтр или выполнили в ней поисковый запрос, то следующая операция фильтрации или поиска будет применена к результатам предыдущей.

11.1. Задача

Проверка и лечение компьютера осуществляется в рамках задачи. К задаче можно перейти, нажав имя задачи в сводной таблице задач на главной странице сервиса.

Задачи имеют *срок действия*, по истечении которого все сформированные отчеты останутся доступны, но новые действия с задачей больше нельзя будет производить. Этот параметр задается при создании пространства и применяется к каждой задаче в рамках пространства. По умолчанию срок действия составляет 10 дней.

Задача, для которой запрошено экспертное сопровождение, становится бессрочной.

Как работать с задачей

1. Создайте задачу.
2. Создайте утилиту FixIt! для сбора данных и отправьте ее владельцу проверяемого компьютера.

   Владелец проверяемого компьютера запускает утилиту на своем компьютере. Утилита проверяет систему и формирует детальный отчет.
3. Получите отчет о состоянии системы. Если отчет не загружается в задачу автоматически, отчет можно загрузить вручную.
4. Проанализируйте отчет в разделе Поиск и анализ.
5. Соберите лечащую утилиту FixIt! для обнаруженных угроз и отправьте ее владельцу проверяемого компьютера.
6. Владелец проверяемого компьютера запускает утилиту. Утилита выполняет заданные команды и формирует детальный отчет.

7. Повторяйте шаги 3–6 до тех пор, пока все угрозы на проверяемом компьютере не будут нейтрализованы.
8. Если компьютер вылечен или проблема перестала быть актуальной, закройте задачу.

Для начала работы создайте новую задачу или перейдите к существующей задаче. После выбора задачи откроется страница задачи.

Информация о задаче

На странице задачи доступна следующая информация:

- имя задачи,
- срок действия,
- создатель,
- дата создания,
- отчеты,
- источник (доступно только для менеджеров и пользователей),
- последнее изменение,
- описание задачи.

Описание задачи может добавить или редактировать администратор или любой участник пространства. Чтобы добавить описание, нажмите кнопку + **Заметка** и введите описание. Чтобы изменить или удалить описание, нажмите ⋮ справа от описания и выберите соответствующую опцию.

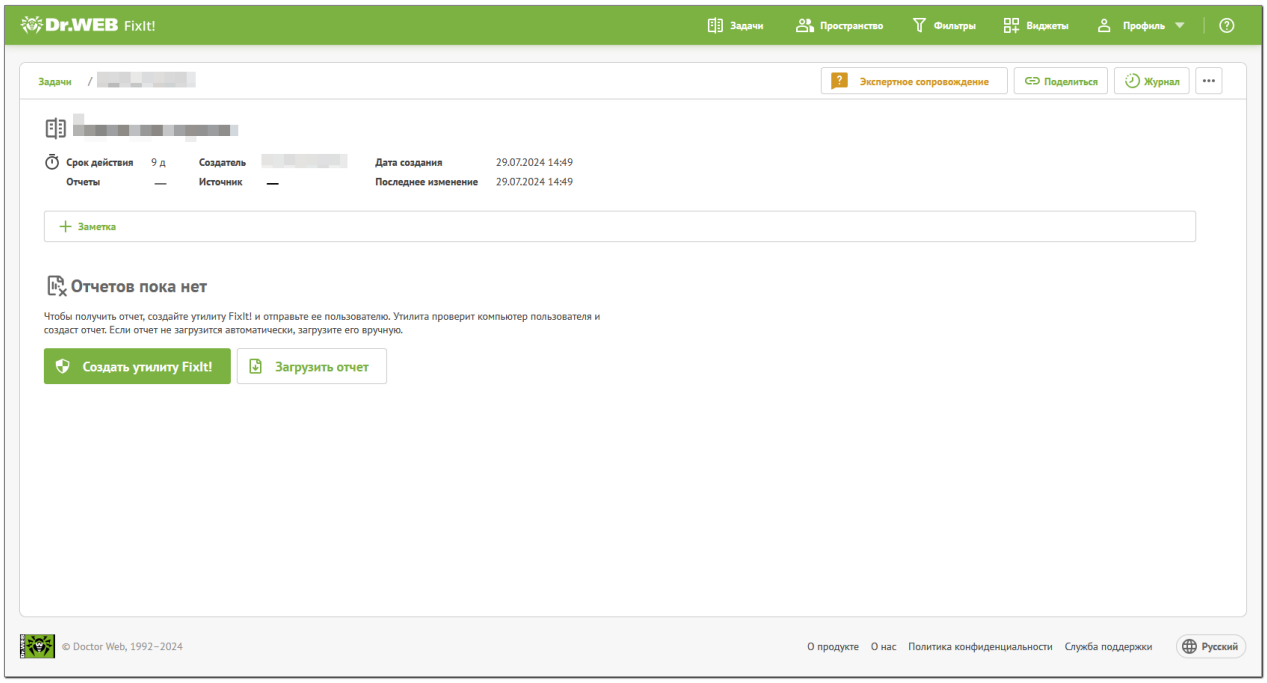

Рисунок 5. Задача

Администратор или любой участник пространства может загрузить отчеты, переименовать, закрыть или переоткрыть любую задачу, а также поделиться задачей со связанным пространством. Администратор или менеджер также может удалить задачу.

Чтобы переименовать задачу

1. Выполните одно из следующих действий:
   - В правом верхнем углу страницы задачи нажмите ••• и выберите **Переименовать**.
   - Наведите курсор на имя задачи и нажмите .
2. Введите новое имя задачи.

Изменения сохранятся автоматически.

Чтобы закрыть задачу

1. В правом верхнем углу страницы задачи нажмите •••.
2. Выберите **Закрыть**.
3. Подтвердите закрытие задачи.

> Закрытые задачи доступны только в режиме для чтения. Переоткройте задачу для возобновления работы.

Чтобы переоткрыть задачу

1. В правом верхнем углу страницы закрытой задачи нажмите .
2. В появившемся окне подтвердите переоткрытие задачи.

Чтобы удалить задачу

1. В правом верхнем углу страницы задачи нажмите ••• и выберите **Удалить**.
2. Подтвердите удаление задачи.

Открытие доступа к задаче

Задачами можно делиться со связанными пространствами для совместной работы.

Чтобы поделиться задачей

1. В правом верхнем углу страницы задачи нажмите кнопку **Поделиться**.
2. На странице **Поделиться** нажмите .

3. В окне **Добавить пространство** выберите пространство, с которым вы хотите поделиться задачей. Администратору при этом будет доступен список всех существующих пространств; менеджеру и пользователю — только связанные пространства.
4. Нажмите **Добавить**.

После того, как вы поделитесь задачей, в вашем списке задач рядом с ней появится значок и она станет доступна в списке задач пространства, с которым вы ей поделились.

При просмотре сведений о задаче имя пространства, которое поделилось задачей, будет отображаться в столбце **Источник**.

Чтобы закрыть доступ к задаче

1. В правом верхнем углу страницы задачи нажмите кнопку **Поделиться**.
2. На странице **Поделиться** в правой части строки с пространством, которому вы хотите закрыть доступ к задаче, нажмите .
3. В окне **Удаление связи** нажмите **Удалить**.

Страница Поделиться

Список пространств, у которых есть доступ к задаче, можно просмотреть и изменить на странице **Поделиться** по нажатию кнопки **Поделиться** на странице задачи.

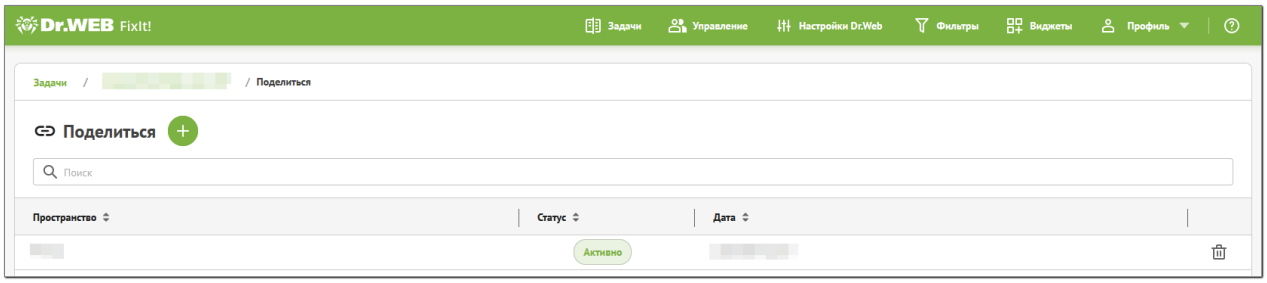

Рисунок 6. Страница Поделиться

В таблице сведений о пространствах, имеющих доступ к задаче, содержится следующая информация:

- пространство,
- статус пространства,
- дата.

Если пространство, с которым вы поделились задачей, будет удалено из списка связанных пространств, то оно потеряет доступ к этой задаче. Вы также потеряете доступ к задачам, которыми с вами поделилось это пространство.

Отчеты

На странице задачи хранятся отчеты о состоянии проверяемого компьютера, полученные в рамках текущей задачи. Отчеты собираются с помощью утилиты FixIt!.

Если в задачу еще не загружены отчеты, необходимо собрать анализирующую утилиту FixIt! и получить отчет или загрузить уже готовый отчет вручную (см. раздел Как загрузить отчет в задачу).

Журнал задач

Сервис Dr.Web FixIt! ведет журнал действий, совершенных с задачами (см. раздел Журнал).

Экспертное сопровождение

Сервис Dr.Web FixIt! позволяет запросить у специалистов компании «Доктор Веб» сопровождение задачи для решения проблемы (см. раздел Экспертное сопровождение).

11.2. Журнал

Журнал содержит записи об изменениях задачи в хронологическом порядке.

Чтобы открыть журнал

1. В списке задач выберите нужную задачу.
2. В правом верхнем углу страницы задачи нажмите **Журнал**.

Записи журнала представлены в табличном виде. Каждая запись содержит следующую информацию:

- **действие**,
- **дата**,
- **источник/инициатор изменения** — пользователь или система,
- **описание**.

Чтобы просмотреть запись, нажмите значок > рядом с нужной записью.

Действия в журнале

События, фиксируемые в журнале, представлены в виде таблицы. В журнале фиксируются:

- Действия с задачами:
  - создание;
  - изменение;
  - запрос экспертного сопровождения — указывается ссылка на страницу запроса, идентификатор запроса и серийный номер сертификата на сопровождение.
- Действия с отчетами:
  - загрузка;
  - переименование;
  - анализ;
  - удаление;
  - скачивание.
- Действия с фильтрами:
  - добавление;
  - изменение;
  - сохранение;
  - удаление.
- Ошибка распознавания файла — текст ошибки выводится во всплывающем окне.
- Действия с утилитой FixIt!:
  - успешное создание — скрипт утилиты выводится во всплывающем окне;
  - ошибка создания — текст ошибки выводится во всплывающем окне;
  - создание анализирующей утилиты;
  - скачивание утилиты.
- Анализ данных отчета:
  - скачивание артефактов отчета, собранных утилитой в соответствии с заданными действиями;
  - скачивание архива с артефактами.
- Действия с виджетами:
  - создание;
  - изменение;
  - удаление;
  - добавление на панель **Виджеты**;
  - удаление с панели **Виджеты**.

Данные таблицы можно упорядочить, нажав значок ▲▼ в нужном столбце таблицы.

Фильтрация и поиск

Для удобства просмотра данных журнала вы можете фильтровать содержимое журнала действий и выполнять поиск по содержимому журнала.

Журнал можно фильтровать по следующим параметрам действия:

- дата,
- источник/инициатор,
- действие.

Чтобы задать фильтр для журнала действий

1. Нажмите над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Источник/Инициатор** или **Действие**:
   - Установите флажки напротив интересующих вас значений и нажмите **Добавить**.

   Если вы выбрали параметр **Дата**:
   - Нажмите интересующие вас даты. Чтобы задать период времени, нажмите дату начала периода и потяните курсор до даты окончания периода. Затем нажмите **Применить**.

Для фильтра можно выбрать только один параметр. Задайте несколько фильтров, чтобы отфильтровать журнал по нескольким параметрам одновременно.

Чтобы выполнить поиск по журналу

1. Введите запрос в поле **Поиск** над таблицей. Поиск выполняется динамически в процессе набора.
2. Нажмите левую кнопку мыши вне поля поиска или клавишу ENTER, чтобы зафиксировать запрос.

Поиск и фильтрация выполняются по данным таблицы в текущем виде. Если вы задали фильтр или выполнили поисковый запрос по журналу, последующая операция фильтрации или поиска будет применена к результатам предыдущей.

Обновление и скачивание журнала

Чтобы обновить журнал, в правом верхнем углу страницы журнала нажмите **Обновить**.

Чтобы скачать журнал, в правом верхнем углу страницы журнала нажмите **Скачать**. Журнал сохраняется в виде файла с расширением .log. Вы сможете открыть его в любом текстовом редакторе.

11.3. Экспертное сопровождение

Если у вас возникли трудности с устранением проблемы, для которой вы завели задачу, доступна возможность запросить *экспертное сопровождение задачи*. В этом случае вы сможете проконсультироваться с аналитиками компании «Доктор Веб» и получить пошаговую поддержку в решении вопроса.

Для получения этой услуги необходимо приобрести сертификат, после активации которого вам будет доступно экспертное сопровождение задачи.

Задача, для которой запрошено экспертное сопровождение, становится *бессрочной*.

Запрос экспертного сопровождения

Чтобы запросить экспертное сопровождение

1. Перейдите на страницу задачи.
2. В правой верхней части страницы нажмите кнопку **Экспертное сопровождение**.
3. В открывшемся окне введите серийный номер сертификата на экспертное сопровождение задачи (см. Рисунок 7). Номер должен быть указан в формате XXXX-XXXX-XXXX-XXXX.
4. Нажмите **Активировать**.

Чтобы приобрести сертификат на экспертное сопровождение

1. Перейдите на страницу задачи.
2. Нажмите кнопку **Экспертное сопровождение** вверху страницы.
3. В открывшемся окне выберите одну из опций:
   - Нажмите **Купить у партнеров**, чтобы приобрести сертификат у партнеров компании «Доктор Веб».
   - Нажмите **Купить онлайн**, чтобы приобрести сертификат в онлайн-магазине компании «Доктор Веб».

Обратите внимание, что при нажатии кнопки **Купить онлайн** генерируется уникальная ссылка, которая действует только один раз. Для повторного перехода в магазин потребуется заново создать ссылку по инструкции выше.

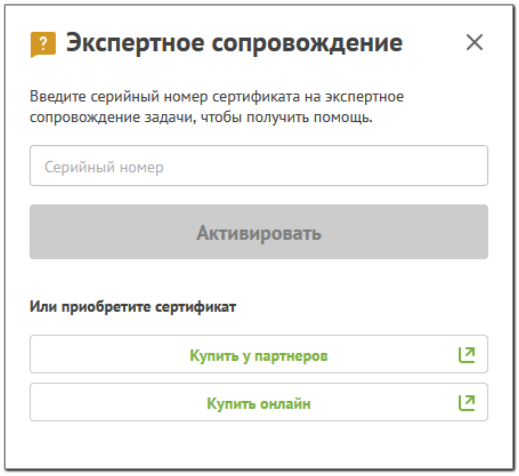

Рисунок 7. Запрос экспертного сопровождения

Страница запроса

После активации сертификата в новой вкладке откроется страница поддержки с вашим запросом. В заголовке запроса указан его идентификатор и статус (новый, подтвержден, ожидание ответа, закрыт).

На этой странице вы можете:

- добавить комментарий;
- закрыть запрос.

Вы будете получать на электронную почту уведомления об изменении статуса вашего запроса и появлении ответов.

Чтобы перейти на страницу существующего запроса

1. Перейдите на страницу соответствующей задачи.
2. В правой верхней части страницы нажмите кнопку **Экспертное сопровождение**.

ИЛИ

1. Перейдите на страницу Журнала задачи.
2. Найдите в таблице строку действия **Экспертное сопровождение** и нажмите >, чтобы развернуть информацию.
3. Перейдите по ссылке в поле **Ссылка на запрос в поддержку**.

ИЛИ

1. Перейдите на страницу пространства.
2. В верхней части страницы нажмите кнопку **Запросы на сопровождение**.
3. Выберите нужный запрос из списка (см. Рисунок 8).
4. Нажмите номер запроса со ссылкой.

ИЛИ

1. Перейдите по ссылке из письма, которое поступит на вашу электронную почту при любом изменении вашего запроса.

Список запросов на сопровождение

Список запросов на сопровождение для всех задач пространства расположен на странице **Запросы на сопровождение**.

Чтобы перейти на страницу Запросы на сопровождение

1. Перейдите на страницу пространства.
2. В верхней части страницы нажмите кнопку **Запросы на сопровождение**.

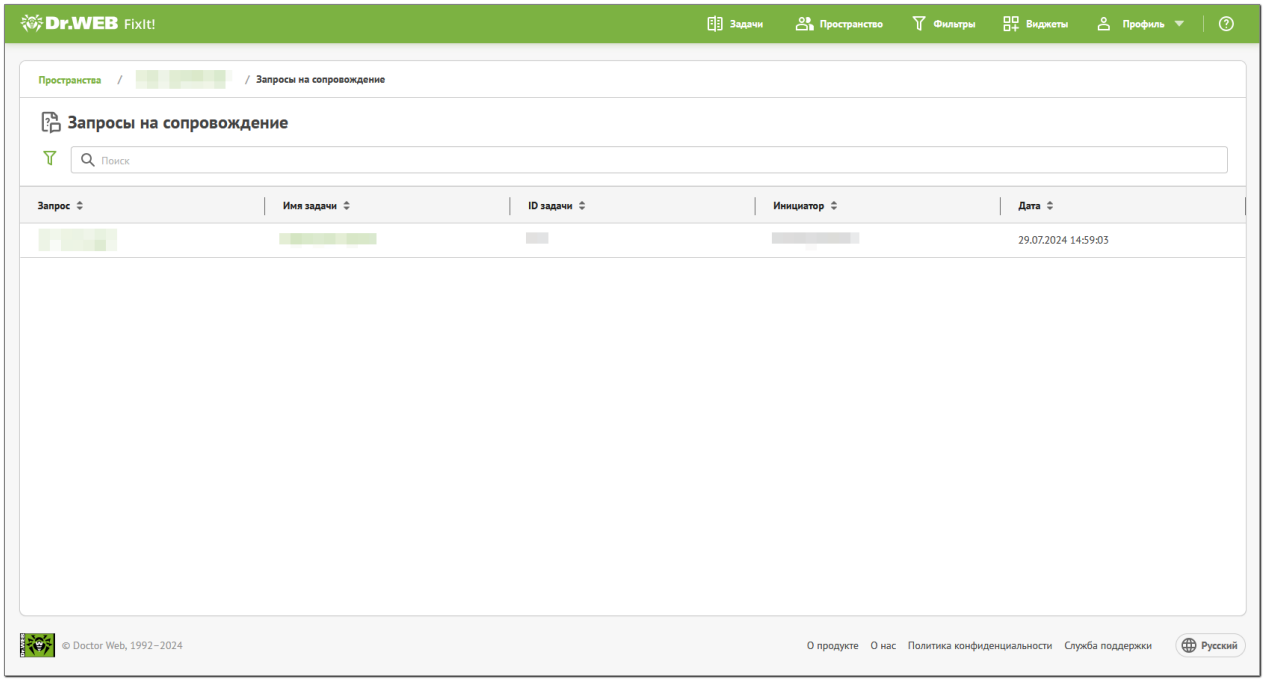

Рисунок 8. Список запросов на сопровождение

В таблице запросов на сопровождение отображается следующая информация:

- идентификатор запроса со ссылкой,
- имя задачи, для которой создан запрос,
- идентификатор задачи,
- инициатор запроса,
- дата запроса.

12. Отчеты

В *отчетах* содержатся подробные сведения о состоянии проверяемого компьютера, собранные утилитой FixIt!. Проанализировав отчет в сервисе, вы сможете создать лечащую утилиту FixIt!, чтобы нейтрализовать найденные угрозы на проверяемом компьютере.

Отчеты можно переименовывать, скачивать и удалять. Кроме того, вы можете сравнить два отчета одной задачи между собой.

Как работать с отчетом

- Загрузите отчет в задачу (это может быть сделано автоматически или вручную).
- Оцените ситуацию на проверяемом компьютере и степень ее опасности, используя виджеты.
- Просмотрите сведения, собранные в рамках отчета.
- При необходимости дополнительно проанализируйте отчет, подключая готовые и созданные самостоятельно фильтры.
- Укажите действия, которые нужно выполнить в отношении различных объектов отчета, например переместить, удалить или вылечить объект.
- Создайте лечащую утилиту FixIt!, которая выполнит на компьютере пользователя действия, указанные вами на предыдущем шаге.

12.1. Как загрузить отчет в задачу

Отчеты могут загружаться в задачу автоматически или вручную. Максимальный размер отчета, который можно загрузить, составляет 12 ГБ.

Чтобы загрузить отчет автоматически

- При сборке утилиты установите переключатель **Автоматически загружать отчеты** (более подробная информация о сборке приведена в разделе Как проверить компьютер утилитой).

Чтобы загрузить отчет вручную

Если в задаче нет загруженных отчетов:

1. Зайдите в задачу.
2. Нажмите кнопку **Загрузить отчет**.

3. Перетащите архив с отчетом в область загрузки или нажмите **Обзор** и выберите архив в Проводнике.
4. Нажмите кнопку **Загрузить**.

Если в задаче есть загруженные отчеты:

1. Зайдите в задачу.
2. Нажмите кнопку рядом с заголовком таблицы **Отчеты**.
3. Перетащите архив с отчетом в область загрузки или нажмите **Обзор** и выберите архив в Проводнике.
4. Нажмите кнопку **Загрузить**.

После загрузки в задачу отчет будет автоматически разобран и подготовлен к анализу, а его данные сгруппированы в категории (см. раздел Данные). При необходимости вы можете повторно разобрать отчет, нажав значок в списке отчетов.

12.2. Общая информация об отчете

Общую информацию об отчете вы можете просмотреть в таблице **Отчеты** на странице задачи. Кроме того, аналогичные сведения приведены на странице самого отчета (вкладка **Об отчете** слева).

Чтобы просмотреть общую информацию об отчете

- В таблице **Отчеты** в задаче
  - Откройте задачу. В таблице **Отчеты** будет приведена общая информация о каждом отчете.
- На странице самого отчета
  - В таблице **Отчеты** нажмите имя отчета. Общая информация об отчете будет приведена в верхней части страницы.

Вы можете узнать следующую общую информацию об отчете:

- **Способ загрузки:** Вручную или Автоматически.
- **Дата создания:** дата формирования отчета.
- **Размер, МБ:** размер файла отчета в мегабайтах.
- **Ключ:** пароль от ZIP-архива с отчетом. Чтобы скопировать ключ, нажмите его.
- **Имя устройства:** имя устройства, при проверке которого был создан отчет.
- **Заметка:** описание отчета. В заметке можно описать цели задачи или фиксировать ход ее решения.

Заметки можно добавлять, редактировать и удалять. Чтобы добавить заметку, нажмите + **Заметка**, введите описание и нажмите **Сохранить**. Чтобы редактировать или удалить заметку, справа от описания нажмите ⋮ и выберите нужную команду.

12.3. Сведения, собранные утилитой FixIt!

Загрузив отчет в задачу, вы можете просмотреть:

- Данные, которые утилита FixIt! собрала на проверяемом компьютере.
- Сведения о системе проверяемого компьютера, полученные утилитой FixIt!.
- Файлы, собранные в процессе проверки компьютера утилитой FixIt!.

12.3.1. Данные

Данные, которые утилита FixIt! собрала на проверяемом компьютере, упорядочены по категориям:

- Dr.Web,
- Приложения,
- Процессы,
- Драйверы,
- Службы,
- Сеть,
- Автозапуск,
- Планировщик заданий,
- Веб-браузеры,
- Журнал событий,
- Реестр,
- Файловая система.

> ⚠ Некоторые категории могут отсутствовать в отчете, если утилита FixIt! не обнаружила их в системе при анализе.

Чтобы просмотреть собранные данные, откройте страницу отчета и выберите на панели слева в выпадающем меню **Данные** нужную категорию.

12.3.1.1. Dr.Web

В разделе **Dr.Web** отображается сводная информация об установленном на устройстве продукте компании «Доктор Веб». На вкладке **Общие** указываются общие сведения, на вкладке **Измененные настройки** — отличия текущих настроек продукта от настроек по

умолчанию, а на вкладке **Карантин** — вредоносные объекты, помещенные продуктом в карантин.

Вкладка Общие

Информация на вкладке **Общие** поделена на сворачивающиеся блоки:

- **О продукте**
- **Установленные компоненты**
- **Установленные продукты**
- **Запущенные модули**
- **Файлы лицензий**
- **Антивирусные базы**
- **Установленное ПО**

Чтобы свернуть такой блок, нажмите значок ▼. Чтобы развернуть его снова, нажмите значок ▶. Данные внутри каждого блока представлены в виде таблицы. Их можно упорядочить, нажав значок ▲▼ в нужном столбце таблицы.

О продукте

В таблице данных этого раздела указаны следующие сведения об установленном программном обеспечении компании «Доктор Веб»:

- **Версия:** версия продукта.
- **Хеш:** хеш-сумма файла программы.
- **Путь:** местоположение папки с файлами программы.
- **Репозиторий:** местоположение репозитория.
- **Путь до баз:** местоположение антивирусных баз.

Установленные компоненты

В таблице данных этого раздела указаны следующие сведения о компонентах антивируса:

- **Имя:** наименование компонента.
- **Статус:** факт установки. Если компонент установлен, то в столбце **Статус** отображается флажок.

Установленные продукты

В таблице данных этого раздела указаны следующие сведения о продуктах компании «Доктор Веб»:

- **Имя:** наименование продукта.
- **Дата создания:** дата создания файла продукта.

Запущенные модули

В таблице данных этого раздела указаны следующие сведения о действующих модулях антивируса:

- **PID:** идентификатор процесса.
- **Имя:** наименование модуля.
- **Версия:** версия модуля.

Файлы лицензий

В таблице данных этого раздела указаны следующие сведения о файлах лицензий программного обеспечения Dr.Web:

- **Имя файла:** наименование файла с лицензией.
- **Номер пользователя:** уникальный номер, присвоенный владельцу лицензии.
- **Имя пользователя:** имя пользователя, владеющего лицензией.
- **Дата создания:** дата и время, когда файл лицензии был создан.
- **Действителен до:** дата и время истечения срока действия лицензии.
- **Устройства:** количество устройств, на которых можно использовать программу согласно лицензии.
- **Приложения:** перечень приложений.
- **Настройки:** перечень компонентов, которые включены или не включены в лицензию.

Чтобы развернуть информацию в ячейке таблицы, нажмите >.

Антивирусные базы

В таблице данных этого раздела указаны следующие сведения о базах вирусных сигнатур, которые антивирус Dr.Web использует для выявления вредоносного кода:

- **Имя файла:** наименование файла с базой вирусных сигнатур.
- **Число записей:** количество записей о сигнатурах в базе.
- **Версия:** версия базы.
- **Unix-время:** дата обновления базы в Unix-формате.
- **Дата:** дата обновления базы.
- **Определяемые угрозы:** тип вредоносных программ, сигнатуры которых содержит база (таких как вирусы, рекламное ПО и др.).

Установленное ПО

В таблице данных этого раздела указаны следующие сведения об установленном продукте Dr.Web:

- **Имя:** наименование продукта Dr.Web.
- **Расположение:** местоположение продукта Dr.Web.
- **Скрипт удаления:** скрипт, с помощью которого можно удалить продукт Dr.Web.

Вкладка Измененные настройки

На этой вкладке отображаются отличия текущих настроек продукта Dr.Web от настроек по умолчанию в виде таблицы со следующими столбцами:

- **Имя:** заданное администратором название настройки.
- **Описание:** информация о настройке.
- **Ключ:** ключ настройки в реестре Windows.
- **Параметр:** имя параметра в реестре Windows.
- **По умолчанию:** значение параметра по умолчанию в реестре Windows.
- **Текущее значение:** текущее значение параметра в реестре Windows.

Вкладка Карантин

На этой вкладке отображаются вредоносные объекты, помещенные в карантин. Объекты приводятся в виде таблицы со следующими столбцами:

- **Объект:** имя объекта.
- **Угроза:** наименование угрозы.
- **Дата добавления:** дата, когда объект был добавлен.
- **Путь:** путь к объекту.
- **Тип:** тип объекта.
- **Компонент:** компонент, который добавил этот объект в карантин.

Вы можете фильтровать таблицу объектов, помещенных в карантин, по типу и компоненту. Для этого нажмите значок  и выберите нужный параметр фильтра.

Кроме того, вы можете выполнять поиск по объектам карантина. Для этого целиком или частично введите имя объекта в строке поиска, расположенной над таблицей.

12.3.1.2. Приложения

Вкладка **Приложения** содержит данные о приложениях, установленных на проверяемом компьютере на момент сбора отчета.

Данные распределены по категориям и представлены в виде сворачивающихся блоков. Чтобы свернуть такой блок, нажмите значок . Чтобы развернуть его снова, нажмите значок .

Категория	Параметры
Установленные приложения	• ID • Имя • Расположение • Удаление • Скрытые
Приложения из магазина Microsoft Store	• Имя • Версия • ID
Приложения MSI	• Имя • Версия • Разработчик

Данные таблиц можно упорядочить, нажав значок в нужном столбце таблицы. Вы также можете выполнить поиск по таблице. Для этого введите запрос в поле **Поиск** над таблицей процессов и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

12.3.1.3. Процессы

Вкладка **Процессы** содержит данные об активных процессах на проверяемом компьютере на момент сбора отчета.

Данные представлены в виде таблицы. Для каждого процесса в таблице указана следующая информация:

- **PID:** идентификатор процесса.
- **Командная строка:** аргументы запуска процесса.
- **Файл:** исполняемый файл процесса.
- **Компания:** издатель исполняемого файла.
- **Подписан:** наличие подписи.
- **Репутация:** оценка потенциального наличия вирусов согласно внутренней базе Metawave, содержащей данные о ранее определенных зараженных файлах.

Каждая строка таблицы Процессы представляет собой сворачивающийся блок, содержащий таблицу файлов, задействованных процессом. В таблице содержатся следующие столбцы данных:

- **Файл**;
- **Компания**;
- **Подписан**;
- **Репутация**.

Вы можете упорядочить строки таблиц по содержимому столбца. Для этого нажмите значок ▲▼ в нужном столбце таблицы.

Вы также можете выполнить поиск по таблице Процессы и всем вложенным таблицам. Для этого введите запрос в поле 🔍 **Поиск** над таблицей Процессы и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

Чтобы посмотреть подробную информацию об определенном процессе или файле из таблицы, нажмите его имя. В правой части экрана появится всплывающее окно **Подробности** со сведениями о параметрах объекта:

Вкладка	Доступные параметры
Процесс	• Статус • Свойства: ▪ PID

Вкладка	Доступные параметры
	▪ Сессия ▪ Адрес ▪ Путь ▪ Командная строка ▪ Текущий каталог ▪ Разрядность ▪ Адрес PEB ▪ Отлажено ▪ Уровень изоляции ▪ Дата создания • Ресурсы: ▪ Kernel time ▪ User time ▪ Приоритет ▪ Handles • Родитель: ▪ PID ▪ Сессия ▪ Путь ▪ Командная строка ▪ Разрядность ▪ Уровень изоляции ▪ Дата создания
Файл	• Путь • Статус: ▪ Сертификат ▪ Файл ▪ Тип ▪ Облако ▪ Тип ПО • Хеш: ▪ SHA1 ▪ SHA256 ▪ Ссылка на сервис VirusTotal • Свойства: ▪ Размер ▪ Дата создания ▪ Последнее изменение

Вкладка	Доступные параметры
	▪ Последнее обращение ▪ Дата сборки • Атрибуты: ▪ Значение ▪ Архив ▪ Безопасность • Версия: ▪ Описание ▪ Версия ▪ Компания ▪ Оригинальное название
Сертификаты	• Статус • Дата и время • Сертификаты: ▪ Субъект ▪ Издатель ▪ Действителен с ▪ Действителен до ▪ Отпечаток SHA1 ▪ Отпечаток SHA256 ▪ Серийный номер ▪ Имя
Данные *(только для файлов)*	• Адрес памяти • Путь • Размер • Статус • Дата сборки

12.3.1.4. Драйверы

Вкладка **Драйверы** содержит информацию о драйверах, обнаруженных на устройстве.

Данные о драйверах представлены в виде сводной таблицы. Таблица содержит следующую информацию:

- **файл**: путь к файлу драйвера;
- **статус**: статус активности драйвера;
- **тип**: тип драйвера;
- **запуск**: кем или как запущен драйвер;

- **компания**: производитель драйвера;
- **подписан**: наличие подписи;
- **репутация**: оценка потенциального наличия вирусов согласно внутренней базе Metawave, содержащей данные о ранее определенных зараженных файлах.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы. Вы также можете выполнить поиск по таблице. Для этого введите запрос в поле **Поиск** над таблицей драйверов и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

Подробную информацию о драйверах можно увидеть, нажав путь к файлу драйвера в таблице. Доступна следующая информация о драйверах:

Вкладка	Доступные параметры
Информация	• путь, • размер, • адрес, • статус.

Файл	• путь;
	• статус:
	  ▪ сертификат,
	  ▪ файл,
	  ▪ тип,
	  ▪ облако,
	  ▪ тип ПО;
	• хеш:
	  ▪ SHA1,
	  ▪ SHA256,
	  ▪ ссылка на сервис VirusTotal;
	• свойства:
	  ▪ размер,
	  ▪ дата создания,

Вкладка	Доступные параметры
	▪ последнее изменение, ▪ последнее обращение, ▪ дата создания; • атрибуты: ▪ значение, ▪ архив, ▪ безопасность; • версия: ▪ описание, ▪ версия, ▪ компания, ▪ оригинальное название.
Сертификаты	• статус; • дата и время; • сертификаты: ▪ субъект, ▪ издатель, ▪ действителен с, ▪ действителен до, ▪ отпечаток SHA1, ▪ отпечаток SHA256, ▪ серийный номер, ▪ имя.

12.3.1.5. Службы

Вкладка **Службы** содержит информацию о службах на проверяемом компьютере.

Данные о службах представлены в виде сводной таблицы. Таблица содержит следующую информацию:

- **имя**: имя службы;
- **запуск**: кем или как запущена служба;
- **состояние**: статус активности службы;
- **PID**: идентификатор процесса службы;
- **командная строка**: путь к файлу службы;
- **подписан**: наличие подписи;
- **репутация**: оценка потенциального наличия вирусов согласно внутренней базе Metawave, содержащей данные о ранее определенных зараженных файлах.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы. Вы также можете выполнить поиск по таблице. Для этого введите запрос в поле **Поиск** над таблицей служб и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

Подробную информацию о службах можно увидеть, нажав имя или путь к службе в таблице. Доступна следующая информация о службах:

Вкладка	**Доступные параметры**
Информация	• статус, • имя, • описание, • тип, • режим запуска, • состояние, • принятые команды, • контроль ошибок, • код выхода, • код выхода Win32, • процесс.

Файл	• путь;
	• статус:
	  ▪ сертификат,
	  ▪ файл,
	  ▪ тип,
	  ▪ облако,
	  ▪ тип ПО;
	• хеш:
	  ▪ SHA1,
	  ▪ SHA256;
	  ▪ ссылка на сервис VirusTotal;
	• свойства:

Вкладка	Доступные параметры
	▪ размер, ▪ дата создания, ▪ последнее изменение, ▪ последнее обращение, ▪ дата создания; • атрибуты: ▪ значение, ▪ архив, ▪ безопасность; • версия: ▪ описание, ▪ версия, ▪ компания, ▪ оригинальное название.
Сертификаты	• статус; • дата и время; • сертификаты: ▪ субъект, ▪ издатель, ▪ действителен с, ▪ действителен до, ▪ отпечаток SHA1, ▪ отпечаток SHA256, ▪ серийный номер, ▪ имя.

12.3.1.6. Сеть

На вкладке **Сеть** представлена информация о сетевых подключениях на проверяемом компьютере.

Данные о подключениях располагаются на вкладках в виде таблиц.

Вкладка	Параметры
Интерфейсы	• Описание • DHCP • Сервер DHCP • IP

Вкладка	Параметры
	• Шлюз • Сервер DNS
Статические маршруты	• Сеть • Маска • Шлюз
Файл HOSTS	• IP • Домены
Подключения	• TCP • UDP • TCPv6 • UDPv6 Данные протоколов представлены в виде вкладок, в каждой из которых содержится таблица со следующими параметрами протокола: • PID • Файл • Компания • Подписан • Репутация • Локальный адрес • Локальный порт • Удаленный адрес • Удаленный порт
Настройки DNS	• Значение • Объект • SID • Ключ
Кеш DNS	• Имя • Узел • Тип • TTL • IPv4 • IPv6
Настройки прокси-сервера	• Значение • Объект • SID • Ключ

Данные таблиц вкладки **Сеть** можно упорядочить, нажав значок ▲▼ в нужном столбце таблицы.

Вы можете выполнить поиск по таблицам данных на вкладке **Подключения**. Для этого введите запрос в поле 🔍 **Поиск** над таблицей данных протокола и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

12.3.1.7. Автозапуск

На вкладке **Автозапуск** доступна информация об автозагрузках на проверяемом компьютере.

Информация об автозагрузках представлена на вкладках, содержащих подробные данные:

Вкладка	Данные
Общие	• WMI: ▪ путь, ▪ пространство имен, ▪ CLSID, ▪ класс, ▪ значение, ▪ рабочий каталог; • провайдеры имен Winsock: ▪ имя, ▪ запуск, ▪ путь, ▪ компания, ▪ подписан, ▪ репутация; • локальные провайдеры имен Winsock: ▪ имя, ▪ запуск,

Вкладка	Данные
	▪ путь, ▪ компания, ▪ подписан, ▪ репутация.
Автозагрузки через реестр	Вкладка содержит список автозагрузок. По нажатию строки автозагрузки разворачивается таблица со следующей информацией об автозагрузке: • ключ, • путь, • компания, • подписан, • репутация.
Ярлыки	Вкладка содержит список ярлыков в системе. По нажатию строки ярлыка разворачивается таблица со следующей информацией о ярлыке: • файл, • команда.

Данные таблиц можно упорядочить, нажав значок ▲▼ в нужном столбце таблицы.

Вы можете выполнить поиск по данным на вкладках **Автозагрузки через реестр** и **Ярлыки**. Для этого введите запрос в поле 🔍 **Поиск** над таблицей данных и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

Подробную информацию можно увидеть, нажав имя файла или путь к файлу в таблице. Доступна следующая информация:

Вкладка	Доступные параметры
Информация	Вкладка **Общие**: • имя,

Вкладка	Доступные параметры
	• состояние, • WOW64, • активен, • GUID, • путь. Вкладка **Автозагрузки через реестр**: • статус, • SID, • ключ, • значение, • объект. Вкладка **Ярлыки**: • статус, • имя, • путь, • аргументы, • объект, • данные.
Файл	• путь; • статус: ▪ сертификат, ▪ файл, ▪ тип, ▪ облако, ▪ тип ПО; • хеш: ▪ SHA1, ▪ SHA256; ▪ ссылка на сервис VirusTotal; • свойства: ▪ размер, ▪ дата создания, ▪ последнее изменение, ▪ последнее обращение, ▪ дата создания; • атрибуты: ▪ значение, ▪ архив,

Вкладка	Доступные параметры
	▪ безопасность; • версия: ▪ описание, ▪ версия, ▪ компания, ▪ оригинальное название.
Сертификаты	• статус; • дата и время; • сертификаты: ▪ субъект, ▪ издатель, ▪ действителен с, ▪ действителен до, ▪ отпечаток SHA1, ▪ отпечаток SHA256, ▪ серийный номер, ▪ имя.

12.3.1.8. Планировщик заданий

Вкладка **Планировщик заданий** содержит список назначенных задач на проверяемом компьютере.

Информация о запланированных задачах представлена в виде таблицы, содержащей следующие данные:

- **имя**: имя запланированной задачи,
- **состояние**: статус запланированной задачи,
- **команда**: команда для выполнения запланированной задачи.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы. Вы также можете выполнить поиск по таблице. Для этого введите запрос в поле **Поиск** над таблицей задач и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

12.3.1.9. Веб-браузеры

Вкладка **Веб-браузеры** содержит данные профилей веб-браузеров, установленных на проверяемом компьютере.

Данные о веб-браузерах представлены в виде вложенных списков с таблицами, содержащими информацию о профилях браузеров. В каждой таблице доступна следующая информация о профиле браузера:

Категория	Параметры
Расширения	• ID, • имя, • путь.
Настройки	• SID, • путь.

Данные таблиц можно упорядочить, нажав значок ▲▼ в нужном столбце таблицы.

Подробные данные о расширениях можно получить, нажав ID нужного расширения; данные о настройках можно получить, нажав SID. По нажатию разворачивается таблица со следующей информацией:

Категория	Подробности
Расширения	• браузер, • статус, • имя, • ID, • версия, • профиль, • SID пользователя, • путь к расположению,

Категория	Подробности
	• URL, • путь, • тип. Для некоторых расширений могут быть доступны данные о файле.
Настройки	• браузер, • статус, • URL, • профиль, • SID, • путь.

12.3.1.10. Журнал событий

На вкладке **Журнал событий** собрана информация о событиях на проверяемом компьютере.

Данные представлены в виде таблицы, содержащей следующую информацию о событиях:

- **ID**: идентификатор события;
- **источник**: источник события;
- **файл**: тип журнала (журнал приложения или системный);
- **компьютер**: имя проверяемого компьютера;
- **дата**: дата события;
- **сообщение**: описание события. Нажмите ›, чтобы раскрыть полный текст описания.

Фильтр и поиск

Для удобства просмотра событий вы можете фильтровать содержимое таблицы и выполнять поиск по ее содержимому.

Таблицу можно фильтровать по следующим параметрам события:

- источник,
- файл,
- компьютер,
- дата.

Чтобы задать фильтр для таблицы событий

1. Нажмите  над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Источник**, **Файл** или **Компьютер**:
   - Установите флажки напротив интересующих вас значений и нажмите **Добавить**.

   Если вы выбрали параметр **Дата**:
   - Нажмите интересующие вас даты. Чтобы задать период времени, нажмите дату начала периода и потяните курсор до даты окончания периода.
4. Нажмите кнопку **Применить**.

Для фильтра можно выбрать только один параметр. Задайте несколько фильтров, чтобы отфильтровать таблицу событий по нескольким параметрам одновременно.

Чтобы выполнить поиск по таблице событий

1. Введите запрос в поле  **Поиск** над таблицей. Поиск выполняется динамически в процессе набора.
2. Нажмите левую кнопку мыши вне поля поиска или клавишу ENTER, чтобы зафиксировать запрос.

Поиск и фильтрация выполняются по данным таблицы в текущем виде. Если вы задали фильтр или выполнили поисковый запрос по таблице, последующая операция фильтрации или поиска будет применена к результатам предыдущей.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

12.3.1.11. Реестр

На вкладке **Реестр** доступна информация о содержимом реестра проверяемого компьютера.

Данные в этой категории имеют два вида представления: список и дерево. По умолчанию данные реестра выводятся в виде списка. Чтобы просмотреть данные в виде дерева, нажмите вкладку **Дерево**.

На вкладке **Список** данные представлены в виде сводной таблицы ключей реестра. В таблице содержится следующая информация:

- **ключ**: полный ключ записи;
- **имя**: имя параметра;
- **тип**: тип параметра;
- **размер**: размер параметра;
- **значение**: значение параметра.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы. Вы также можете выполнить поиск по таблице. Для этого введите запрос в поле **Поиск** над таблицей и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

Нажмите ключ реестра в списке или имя параметра в дереве, чтобы увидеть более подробную информацию. Доступны следующие данные о содержимом реестра:

Вкладка	Данные
Информация	• SID, • ключ, • подключ, • последний доступ, • безопасность, • статус.
Значение	Параметры представлены в виде раскрывающегося списка. Для каждого параметра доступны: • имя, • тип, • размер, • значение, • статус.

12.3.1.12. Файловая система

Вкладка **Файловая система** содержит информацию о файловой системе проверяемого компьютера.

Данные в этой категории имеют два вида представления: список и дерево. По умолчанию файловая система представлена в виде списка. Чтобы просмотреть данные в виде дерева, нажмите вкладку **Дерево**.

На вкладке **Список** данные представлены в виде сводной таблицы файлов. В таблице содержится следующая информация о файлах:

- **имя**: путь к файлу,
- **SHA1**: хеш-сумма файла,
- **подписан**: наличие подписи,
- **размер**: размер файла,
- **последнее изменение**: дата и время последнего изменения,
- **репутация**: оценка потенциального наличия вирусов согласно внутренней базе Metawave, содержащей данные о ранее определенных зараженных файлах.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы. Вы также можете выполнить поиск по таблице. Для этого введите запрос в поле **Поиск** над таблицей и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

Подробную информацию о файлах можно увидеть, нажав путь к файлу в таблице на вкладке **Список** или имя файла в дереве на вкладке **Дерево**. В зависимости от типа файла доступна следующая информация:

Вкладка	Доступные параметры

Файл	• путь;
	• статус:
	  ▪ сертификат,
	  ▪ файл,

Вкладка	Доступные параметры
	▪ тип, ▪ облако, ▪ тип ПО; • хеш: ▪ SHA1, ▪ SHA256, ▪ ссылка на сервис VirusTotal; • свойства: ▪ размер, ▪ дата создания, ▪ последнее изменение, ▪ последнее обращение, ▪ дата создания; • атрибуты: ▪ значение, ▪ архив, ▪ безопасность; • версия: ▪ описание, ▪ версия, ▪ компания, ▪ оригинальное название.
Сертификаты	• статус; • дата и время; • сертификаты: ▪ субъект, ▪ издатель, ▪ действителен с, ▪ действителен до, ▪ отпечаток SHA1, ▪ отпечаток SHA256, ▪ серийный номер, ▪ имя.

12.3.2. Система

Сведения о системе проверяемого компьютера, полученные утилитой FixIt!, упорядочены по категориям и представлены в виде минипанелей.

Категория	Что отображается на минипанели
Процессоры	• текущая частота процессора (в % и ГГц), • имя, • описание (во всплывающей подсказке), • максимальная частота, ГГц, • базовая частота, ГГц, • количество физических ядер, • количество логических ядер.
Оперативная память	• использованный/общий объем локальной памяти, • использованный/общий объем виртуальной памяти.
Индекс производительности	• средний балл (рассчитывается на основе оценок по пяти приведенным ниже параметрам), • оценка по параметру Оперативная память, • оценка по параметру Процессор, • оценка по параметру Диск, • оценка по параметру 3D-графика, • оценка по параметру Графика.
ОС	• название, • версия, • папка, • имя устройства, • тип системы, • режим загрузки, • время работы, • местное время.
Антивирус и брандмауэр	• продукт, • версия, • статус, • компания.
Локализация	• страна или регион, • часовой пояс, • язык ОС, • язык интерфейса.
Жесткие диски	Информация о жестких дисках представлена в виде раскрывающихся блоков. В заголовке блока указывается: • название жесткого диска, • занятый/общий объем. В самих блоках приводится следующая информация о каждом жестком диске:

Категория	Что отображается на минипанели
	• диск (указывается буква диска), • серийный номер, • свободное место, ГБ, • файловая система, • метка. Нажав в правой части заголовка раскрывающегося блока кнопку **S.M.A.R.T.**, вы сможете посмотреть характеристики конкретного диска во всплывающем окне.
Учетные записи	• имя, • роль, • описание и группа (во всплывающей подсказке).
Сетевой диск	• имя пользователя, • удаленный каталог, • имя провайдера, • буква диска.
Ярлык сетевого ресурса	• имя пользователя, • имя, • путь.
Переменные среды	• имя, • путь.

Чтобы просмотреть полученные сведения о системе, откройте страницу отчета и выберите на панели слева вкладку **Система**.

12.3.3. Файлы

Файлы, собранные в процессе проверки компьютера утилитой FixIt!, отображаются в виде таблицы на вкладке **Файлы** страницы отчета. Таблица включает указанные ниже столбцы.

Название столбца	Содержимое
Файл	Название файла
SHA1	Алгоритм криптографического хеширования файла
Размер, КБ	Размер файла в килобайтах
Последнее изменение	Дата изменения файла
Репутация	Результат проверки файла во внутреннем сервисе Metawave

Значками в таблице обозначены следующие опции:

- — скачать файл;
- — открыть страницу файла на портале VirusTotal.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы.

Проверка файлов

Вы можете запустить проверку файлов по репутационной базе.

Репутация определяет статус файла. Допустимые значения: вредоносный, подозрительный, подозрительный поставщик, неизвестный, не найденный, доверенный.

Вы можете запустить повторную проверку файла, нажав значок .

Если в ходе проверки файла возникнет ошибка, появится статус **Ошибка**.

Поиск

Вы можете искать нужные вам файлы в таблице. Для этого введите запрос в поле **Поиск** и нажмите ENTER.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

Скачивание файлов

Вы можете скачать файлы этого раздела на свое устройство.

- Чтобы скачать файл, в строке таблицы нажмите .
- Чтобы скачать сразу несколько файлов, установите флажки рядом с нужными файлами и нажмите над таблицей кнопку **Скачать**.

12.4. Как посмотреть список отчетов

Если в задачу был загружен хотя бы один отчет, на странице задачи располагается сводная таблица всех отчетов текущей задачи. Для каждого отчета доступна следующая информация:

- **ID**: числовой идентификатор отчета внутри задачи. Генерируется автоматически.
- **Имя**: имя отчета. Генерируется автоматически. Впоследствии имя отчета можно поменять.
- **Статус**: стадия анализа отчета.
- **Способ загрузки**: автоматически или вручную.
- **Дата загрузки**.

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы.

Фильтрация и поиск

Для удобства просмотра информации об отчетах задачи вы можете фильтровать содержимое сводной таблицы отчетов и выполнять поиск по содержимому таблицы.

Таблицу можно фильтровать по следующим параметрам отчета:

- способ загрузки,
- дата загрузки.

Чтобы задать фильтр для таблицы отчетов

1. Нажмите над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Способ загрузки**:
   - Установите флажки напротив интересующих вас значений и нажмите **Добавить**.

   Если вы выбрали параметр **Дата загрузки**:
   - Нажмите интересующие вас даты. Чтобы задать период времени, нажмите дату начала периода и потяните курсор до даты окончания периода. Затем нажмите **Применить**.

Для фильтра можно выбрать только один параметр. Задайте несколько фильтров, чтобы отфильтровать таблицу отчетов по нескольким параметрам одновременно.

Чтобы выполнить поиск по таблице отчетов

1. Введите запрос в поле **Поиск** над таблицей. Поиск выполняется динамически в процессе набора.

2. Нажмите левую кнопку мыши вне поля поиска или клавишу ENTER, чтобы зафиксировать запрос.

Поиск и фильтрация выполняются по данным таблицы в текущем виде. Если вы задали фильтр или выполнили поисковый запрос по таблице, последующая операция фильтрации или поиска будет применена к результатам предыдущей.

Для просмотра и дальнейшей работы с отчетом нажмите его имя в таблице отчетов.

12.5. Как сравнить отчеты

Если задача содержит более одного отчета, вы можете сравнить отчеты, созданные в разное время, чтобы выявить различия в состоянии системы на момент получения отчетов, в том числе исправление выявленных ранее проблем и появление новых.

Чтобы сравнить отчеты

1. В правом верхнем углу вкладки **Об отчете** нажмите кнопку **Сравнить** .
2. На странице **Сравнение отчетов** в выпадающем списке выберите пару отчетов для сравнения.

Чтобы поменять отчеты местами, нажмите значок .

Таблица Сравнение отчетов

В таблице на странице **Сравнение отчетов** доступна следующая информация о сравниваемых объектах из отчетов:

- **Путь**: путь к объекту сравнения на проверяемом компьютере.
- **Статус**: Изменено, Новое или Удалено.
- **Тип**: категория объекта в отчете.

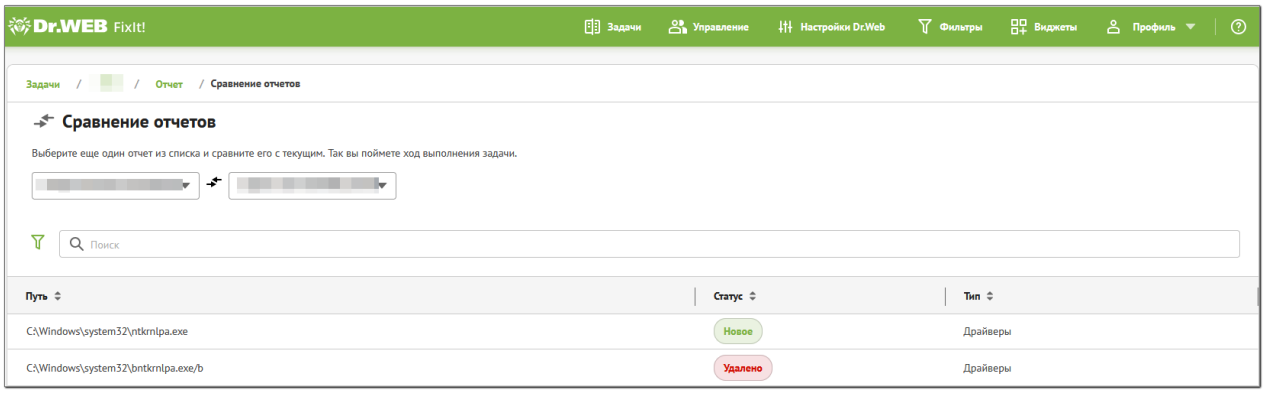

Рисунок 9. Сравнение отчетов

Данные таблицы можно упорядочить, нажав значок в нужном столбце таблицы.

Фильтрация и поиск

Для удобства просмотра данных сравниваемых отчетов вы можете фильтровать содержимое таблицы сравниваемых объектов и выполнять поиск по содержимому таблицы.

Таблицу можно фильтровать по следующим параметрам объекта:

- статус,
- тип.

Чтобы задать фильтр для таблицы сравниваемых объектов

1. Нажмите над таблицей.
2. Выберите параметр фильтрации.
3. Установите флажки напротив интересующих вас значений.
4. Нажмите **Применить**.

Для фильтра можно выбрать только один параметр. Задайте несколько фильтров, чтобы отфильтровать таблицу объектов по нескольким параметрам одновременно.

Чтобы выполнить поиск по таблице сравниваемых объектов

1. Введите запрос в поле **Поиск** над таблицей. Поиск выполняется динамически в процессе набора.
2. Нажмите левую кнопку мыши вне поля поиска или клавишу ENTER, чтобы зафиксировать запрос.

Поиск и фильтрация выполняются по данным таблицы в текущем виде. Если вы задали фильтр или выполнили поисковый запрос по таблице, последующая операция фильтрации или поиска будет применена к результатам предыдущей.

FixIt! позволяет выполнять поиск по частичному совпадению. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

12.6. Как скачать отчет

Вы можете скачивать отчеты в формате ZIP на свой компьютер.

Чтобы скачать отчет

- Через таблицу **Отчеты** в задаче
  1. В правой части строки отчета нажмите .
     Вы можете скачивать отчет, даже когда он анализируется: во время анализа значок остается доступным.
- На странице отчета
  1. В таблице **Отчеты** нажмите имя отчета.
  2. В правом верхнем углу страницы отчета выберите ··· > **Скачать**.

12.7. Как переименовать отчет

Вы можете изменить имя отчета, выбрав другое, более понятное для вас название.

Чтобы переименовать отчет

1. На странице отчета выполните одно из следующих действий:
   - В правом верхнем углу вкладки **Об отчете** нажмите ··· > **Переименовать**.
   - Наведите курсор на имя отчета и нажмите .
2. Введите новое имя отчета и нажмите ENTER.

12.8. Как удалить отчет

Требуется роль администратора или менеджера.

Чтобы удалить отчет

1. Перейдите на страницу отчета.
2. Нажмите ··· > **Удалить**.
3. Подтвердите удаление.

13. Виджеты

Используя виджеты, вы можете быстро оценить ситуацию, возникшую на проверяемом компьютере, и степень ее опасности.

Виджеты представляют собой минипанели с набором фильтров, автоматически применяемых к отчету. Изучив, сколько и какие именно фильтры сработали при анализе отчета, вы сможете быстро понять, что происходит на проверяемом компьютере. Вы можете использовать для анализа предустановленные виджеты, созданные администратором, а также создавать собственные виджеты, если, например, хотите провести собственный дополнительный анализ. Вы можете выключать ненужные виджеты, показывать только виджеты с определенным уровнем опасности или отображать виджеты, созданные для конкретной задачи. Это позволит вам легко выбирать нужные виджеты для конкретных задач.

Управление виджетами

Для управления виджетами пространства используйте панель **Виджеты**. На ней удобно просматривать виджеты в виде списка, а также изменять и удалять их. Чтобы открыть панель **Виджеты**, на верхней панели FixIt! нажмите **Виджеты**.

Если вы хотите поработать с виджетами, доступными только в рамках отдельной задачи, перейдите в раздел **Виджеты** отчета. Для этого:

1. Откройте панель **Задачи**.
2. Выберите в списке нужную задачу.
3. Откройте отчет, обзорную информацию по которому вы хотите получить.
4. На боковой панели слева нажмите **Виджеты**.

13.1. Как анализировать отчет с помощью виджетов

Используя виджеты, вы можете быстро проанализировать полученный отчет и оценить состояние компьютера пользователя.

Чтобы проанализировать отчет с помощью виджетов

1. Откройте панель **Задачи**.
2. Выберите в списке нужную задачу.
3. Откройте отчет, который хотите проанализировать.
4. На боковой панели слева нажмите **Виджеты**.

5. На вкладке **Все виджеты** оцените результаты применения к отчету различных фильтров. Это удобно сделать визуально по значкам степени опасности: Угроза, Подозрительно и Инфо.

Далее при желании вы можете фильтровать виджеты по степени опасности, просматривать подробную информацию по сработавшим фильтрам определенного виджета и перезапускать анализ с использованием фильтров определенного виджета.

13.2. Категории виджетов

Виджеты делятся на категории по уровню доступности для пользователей:

Категория	Описание	Доступные действия
Для всех	Предустановленные виджеты.	Участники пространства могут только включать и выключать их. **Примечание.** Администратор может защищать виджеты этой категории от выключения. Защищенный виджет будет всегда включен.
Для пространства	Виджеты, которые могут использоваться только внутри определенного пространства.	Участники пространства могут включать, выключать, изменять и удалять их.
Для задачи	Виджеты, которые могут использоваться только внутри определенной задачи.	Участники пространства могут включать, выключать, изменять и удалять их.
Для меня	Виджеты, которые видит только его автор.	Такой виджет может включать, выключать, изменять и удалять только его автор.

Кроме того, виджеты различаются по составу: они могут включать в себя только отдельные фильтры или только группы фильтров.

13.3. Как посмотреть список виджетов

Вы можете смотреть списки виджетов отдельных категорий.

Чтобы посмотреть список виджетов категории Для всех

1. На верхней панели FixIt! нажмите **Задачи**.
2. Выберите в списке любую задачу, а затем любой отчет этой задачи.
3. На боковой панели слева нажмите **Виджеты**.

4. В правом верхнем углу панели **Виджеты** нажмите **Все виджеты**.
5. В окне **Все виджеты** на боковой панели слева выберите категорию **Для всех**. В центральной части окна отобразится список всех виджетов этой категории.

Чтобы посмотреть список виджетов категории Для пространства

Вы можете посмотреть список виджетов категории **Для пространства** двумя способами.

- В окне **Все виджеты** (внутри отчета). Для этого:
  1. На верхней панели FixIt! нажмите **Задачи**.
  2. Выберите в списке любую задачу, а затем любой отчет этой задачи.
  3. На боковой панели слева нажмите **Виджеты**.
  4. В правом верхнем углу панели **Виджеты** нажмите **Все виджеты**.
  5. В окне **Все виджеты** на боковой панели слева выберите категорию **Для пространства**. В центральной части окна отобразится список всех виджетов этой категории.
- На панели **Виджеты**. Для этого:
  1. На верхней панели FixIt! нажмите **Виджеты**.
  2. На открывшейся панели **Виджеты** перейдите на вкладку **Для пространства**.

Чтобы посмотреть список виджетов категории Для задачи

1. На верхней панели FixIt! нажмите **Задачи**.
2. Выберите в списке любую задачу, а затем любой отчет этой задачи.
3. На боковой панели слева нажмите **Виджеты**.
4. В правом верхнем углу панели **Виджеты** нажмите **Все виджеты**.
5. В окне **Все виджеты** на боковой панели слева выберите категорию **Для задачи**. В центральной части окна отобразится список всех виджетов этой категории.

Чтобы посмотреть список виджетов категории Для меня

Вы можете посмотреть список виджетов категории **Для меня** двумя способами:

- В окне **Все виджеты** (внутри отчета)
  1. На верхней панели FixIt! нажмите **Задачи**.
  2. Выберите в списке любую задачу, а затем любой отчет этой задачи.
  3. На боковой панели слева нажмите **Виджеты**.
  4. В правом верхнем углу панели **Виджеты** нажмите **Все виджеты**.

5. В окне **Все виджеты** на боковой панели слева выберите категорию **Для меня**. В центральной части окна отобразится список всех виджетов этой категории.

- На панели **Виджеты**

1. На верхней панели FixIt! нажмите **Виджеты**.
2. На открывшейся панели **Виджеты** откройте вкладку **Для меня**.

13.4. Как создать виджет

Вы можете создавать собственные виджеты, добавляя в них нужные вам фильтры или группы фильтров.

Чтобы создать виджет

1. Откройте окно **Новый виджет**. Сделать это можно одним из двух способов:

- Из отчета

a. На верхней панели FixIt! нажмите **Задачи**.

b. Выберите в списке любую задачу, а затем любой отчет этой задачи.

> Если вы хотите создать виджет категории **Для задачи**, то вам нужно выбрать не любую задачу, а определенную.

c. На боковой панели слева нажмите **Виджеты**.

d. На панели **Виджеты** нажмите .

- Из панели **Виджеты** в главном окне

a. На верхней панели FixIt! нажмите **Виджеты**.

b. В верхней части вкладки **Виджеты** нажмите .

2. В выпадающем списке **Доступно** выберите категорию виджета: **Для пространства**, **Для задачи** или **Для меня**.

> Категория **Для задачи** отображается в списке, только если вы создаете виджет из отчета.

3. В выпадающем списке **Тип** выберите тип виджета (виджеты могут состоять из фильтров или групп фильтров).
4. Нажмите **Добавить** и укажите фильтры или группы фильтров, которые должны использоваться в этом виджете.

5. Введите имя виджета.
6. Задайте уровень опасности для виджета. В дальнейшем вы сможете фильтровать и сортировать виджеты по этому уровню.
7. (Необязательно) Введите описание виджета.
8. Нажмите **Создать**.

Созданные виджеты автоматически применятся к отчету, когда вы откроете его вкладку **Виджеты**. Это позволяет анализировать с помощью новых виджетов даже те отчеты, которые были созданы раньше, чем эти виджеты.

13.5. Как изменить виджет

Вы можете изменять любые виджеты, кроме предустановленных (то есть виджетов категории **Для всех**).

Чтобы изменить виджет категории Для пространства или Для меня

1. На верхней панели FixIt! нажмите **Виджеты**.
2. Наведите курсор мыши на имя виджета в списке и нажмите значок .
3. Измените настройки виджета и нажмите **Сохранить**.

Чтобы изменить виджет категории Для задачи

1. На верхней панели FixIt! нажмите **Задачи**.
2. Выберите в списке задачу, виджет которой нужно изменить, а затем любой отчет этой задачи.
3. На боковой панели слева нажмите **Виджеты**. Отобразится панель **Виджеты** для этого отчета.
4. Перейдите на вкладку **Для задачи**.
5. В правом верхнем углу минипанели виджета, который вы хотите изменить, нажмите ··· > **Изменить**.
6. Измените настройки виджета и нажмите **Сохранить**.

13.6. Как включить или выключить виджет

Вы можете выключать виджеты, которые вам не нужны, и включать их снова.

Некоторые виджеты категории **Для всех** могут быть защищены от выключения. Такие виджеты будут всегда включены.

Чтобы включить виджет

1. На верхней панели FixIt! нажмите **Задачи**.
2. Выберите в списке задачу, виджет которой нужно включить, а затем любой отчет этой задачи.
3. На боковой панели слева нажмите **Виджеты**.
4. В правом верхнем углу панели **Виджеты** нажмите **Все виджеты**.
5. В окне **Все виджеты** на боковой панели слева выберите категорию виджета, который нужно включить.
6. В центральной части окна нажмите нужный виджет.
7. В правой части окна установите переключатель **Включить**. Виджет будет включен и появится на панели **Виджеты** в отчете.

Чтобы выключить виджет

1. На верхней панели FixIt! нажмите **Задачи**.
2. Выберите в списке задачу, виджет которой нужно выключить, а затем любой отчет этой задачи.
3. На боковой панели слева нажмите **Виджеты**.
4. При желании перейдите на вкладку нужной категории виджетов.
5. Чтобы выключить виджет категории **Для всех**, **Для пространства** или **Для меня**, в правом верхнем углу минипанели этого виджета нажмите . Чтобы выключить виджет категории **Для задачи**, в правом верхнем углу минипанели этого виджета нажмите ··· > **Выключить**.

13.7. Как удалить виджет

Вы можете удалять любые виджеты, кроме предустановленных (то есть виджетов категории **Для всех**).

Чтобы удалить виджет категории Для пространства или Для меня

1. На верхней панели FixIt! нажмите **Виджеты**.
2. Найдите виджет, который хотите удалить. В правой части строки этого виджета нажмите .
3. Нажмите **Удалить**.

Чтобы удалить виджет категории Для задачи

1. На верхней панели FixIt! нажмите **Задачи**.

2. Выберите в списке задачу, виджет которой нужно изменить, а затем отчет этой задачи.
3. На боковой панели слева нажмите **Виджеты**. Отобразится панель **Виджеты** для этого отчета.
4. Перейдите на вкладку **Для задачи**.
5. В правом верхнем углу минипанели виджета, который вы хотите изменить, нажмите ··· > **Удалить**.
6. Подтвердите удаление, нажав **Удалить**.

13.8. Как узнать состав виджета

В состав виджета могут входить только фильтры или только группы фильтров.

Чтобы узнать состав виджета

- В окне **Все виджеты**
  1. На верхней панели FixIt! нажмите **Задачи**.
  2. Выберите в списке задачу, а затем отчет этой задачи.
  3. На боковой панели слева нажмите **Виджеты**. Отобразится панель **Виджеты** для этого отчета.
  4. В правом верхнем углу панели **Виджеты** нажмите **Все виджеты**.
  5. В центральной части окна **Все виджеты** выберите нужный виджет.
  6. Информация о составе виджета отобразится в правой части окна.
- На панели **Поиск и анализ**
  1. На верхней панели FixIt! нажмите **Задачи**.
  2. Выберите в списке задачу, а затем отчет этой задачи.
  3. На боковой панели слева нажмите **Виджеты**. Отобразится панель **Виджеты** для этого отчета.
  4. В нужном виджете нажмите **Подробнее**.
  5. Откроется панель **Поиск и анализ**, в которой будут отображаться все фильтры из этого виджета.

> Если ни один из фильтров в виджете не сработал, кнопка **Подробнее** в нем будет недоступна. В таком случае используйте первый способ для определения состава виджета.

13.9. Как управлять виджетами

Вы можете выполнять поиск виджетов по имени, сортировать их, а также фильтровать по категории (Для всех, Для меня и т. д.) и уровню опасности.

Как выполнять поиск виджета

Вы можете искать виджеты по имени. Для удобства и скорости поиск будет выполняться по мере ввода символов в строке поиска.

Чтобы выполнить поиск виджета

1. На верхней панели FixIt! нажмите **Виджеты**.
2. Выберите вкладку с категорией виджетов: **Все виджеты**, **Для пространства** или **Для меня**.
3. В строке поиска введите имя виджета целиком или частично.

> Будьте внимательны, выбирая перед поиском вкладку с категорией виджетов. Если, например, вы перейдете на вкладку **Для меня**, то поиск будет выполняться только среди виджетов с этой категории. Чтобы выполнить поиск среди всех виджетов, перейдите на вкладку **Все виджеты**.

Как сортировать виджеты

Вы можете сортировать виджеты по имени, категории, уровню опасности и типу.

Чтобы отсортировать виджеты

1. На верхней панели FixIt! нажмите **Виджеты**.
2. Выберите вкладку с категорией виджетов: **Все виджеты**, **Для пространства** или **Для меня**.
3. Чтобы отсортировать виджеты по определенному столбцу, нажмите заголовок этого столбца. Чтобы изменить порядок сортировки на противоположный, нажмите заголовок еще раз.

Как фильтровать виджеты

Вы можете фильтровать виджеты по категории (Для всех, Для меня и т. д.) и уровню опасности (Опасно, Подозрительно, Инфо).

Чтобы отфильтровать виджеты по категории

- Из панели **Виджеты** в главном окне:
  1. На верхней панели FixIt! нажмите **Виджеты**.
  2. Выберите вкладку с нужной категорией виджетов: **Все виджеты**, **Для пространства** или **Для меня**.
- Из отчета:
  1. На верхней панели FixIt! нажмите **Задачи**.
  2. Выберите в списке задачу, а затем отчет этой задачи.
  3. На боковой панели слева нажмите **Виджеты**. Отобразится панель **Виджеты** для этого отчета.
  4. Выберите вкладку с нужной категорией виджетов: **Все виджеты**, **Для пространства**, **Для задачи** или **Для меня**.

Чтобы отфильтровать виджеты по уровню опасности

- Из панели **Виджеты** в главном окне:
  1. На верхней панели FixIt! нажмите **Виджеты**.
  2. Активируйте переключатель справа от строки поиска.
  3. Выберите уровень опасности на панели справа от переключателя.

  Чтобы сбросить фильтр по уровню опасности, выключите переключатель.
- Из отчета:
  1. На верхней панели FixIt! нажмите **Задачи**.
  2. Выберите в списке задачу, а затем отчет этой задачи.
  3. На боковой панели слева нажмите **Виджеты**. Отобразится панель **Виджеты** для этого отчета.
  4. Активируйте переключатель в правой верхней части панели **Виджеты**.
  5. Выберите уровень опасности на панели справа от переключателя.

  Чтобы сбросить фильтр по уровню опасности, выключите переключатель.

14. Поиск и анализ

Раздел **Поиск и анализ** служит для анализа данных отчета. Вы можете выполнить поисковые запросы с помощью фильтров, применить действия к вредоносным объектам и создать лечащую утилиту FixIt! для исправления выявленных проблем.

Раздел включает в себя вкладки:

- Готовые фильтры
- Новый фильтр
- Выбранные действия

14.1. Готовые фильтры

На вкладке **Готовые фильтры** вы можете выбирать и применять для анализа отчета фильтры, созданные ранее вами или другими пользователями.

Все готовые фильтры систематизированы по категориям:

- **Для всех.** Фильтры, доступны всем пользователям сервиса.
- **Для меня.** Фильтры, доступные только вам.
- **Для этого пространства.** Фильтры, доступные участникам пространства.
- **Для текущей задачи.** Фильтры, доступные только из задачи.

Чтобы выбрать готовый фильтр

1. На вкладке **Готовые фильтры** нажмите **Добавить**. Откроется окно **Добавить фильтры**, в котором будут отображаться все готовые фильтры, систематизированные по категориям, а также готовые фильтры, которые вы добавили в избранное.
2. Выберите нужные вам фильтры и нажмите **Добавить**.

Чтобы быстро найти в окне **Добавить фильтры** нужный вам фильтр, используйте строку поиска.

Результаты поиска по фильтру

Данные отчета, соответствующие примененным фильтрам, отображаются под списком этих фильтров. Данные представлены в виде сворачивающихся блоков со списками найденных объектов. Каждый блок со списком соответствует одному фильтру. Если данные, соответствующие фильтру, не найдены, блок не отображается.

Внутри каждого сворачивающегося блока находится таблица с данными, найденными в отчете с помощью фильтра. В таблицу входят следующие столбцы:

- **Тип:** тип объекта.
- **Действие:** действие, которое будет применено к выбранному объекту.

Остальные столбцы таблицы представляют собой поля, заданные в фильтре.

Действия

Для каждого найденного фильтром объекта можно выбрать действие, которое будет применено к нему лечащей утилитой FixIt!. С помощью действий вы можете устранить проблемы на проверяемом компьютере. Для разных типов объектов доступны разные действия.

Доступные действия перечислены в виде выпадающего списка в столбце **Действие** в таблице результатов поиска по фильтру.

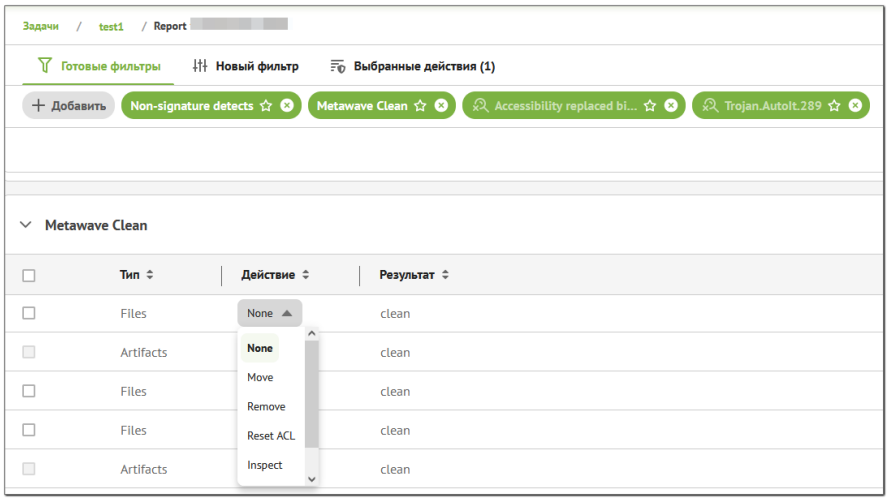

Рисунок 10. Выбор действия для файла

Чтобы выбрать сразу несколько объектов, отметьте их флажками. Чтобы выбрать сразу все объекты на текущей странице в таблице фильтра, отметьте флажком заголовок столбца.

При выборе объектов над таблицей появляется меню выбора группового действия.

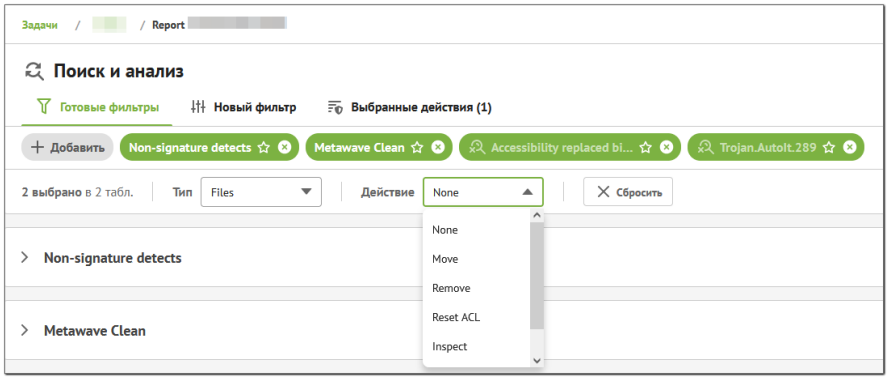

Рисунок 11. Выбор группового действия

Чтобы выбрать действие для нескольких объектов

1. Отметьте нужные объекты флажками. Объекты можно отмечать сразу в нескольких таблицах.
2. Выберите тип объекта в выпадающем меню **Тип** над таблицами (если выбраны объекты нескольких типов).
3. Выберите нужное действие в выпадающем меню **Действие**.
4. Повторите для каждого типа объекта (ваш выбор сохранится).

   Чтобы снять все флажки с выбранных объектов, нажмите кнопку **Сбросить**.

> Обратите внимание: если вы уже выбрали действия для объектов, при сбросе флажков ваш выбор сохранится.

В таблице ниже перечислены все доступные действия над объектами с описанием.

Действие	Описание	Тип объекта
Move	Переместить или переименовать объект	Files
Remove	Удалить объект	Files, mium Extensions, Registry, Shortcuts, Firefox add-ons
Reset ACL	Установить родительский ACL для файла или каталога	Files, Registry
Inspect	Собрать дополнительную информацию об объекте	Files, Processes, Drivers, Registry
Disinfect	Вылечить объект	Files, Registry startups, Registry, Non-signature

Действие	Описание	Тип объекта
		detections, DNS settings, Internet Explorer settings, Proxy settings
Execute	Запустить процесс	Processes
Kill	Завершить процесс	
Suspend	Заморозить процесс	
Start	Запустить службу	Services
Stop	Остановить службу	
Control	Отправить управляющий код службе	
Delete	Удалить объект	Services, Scheduled tasks, Namespace service providers, Layered service providers, WMI providers, WMI
Clear	Закомментировать ("#" + line) указанные строки из файла HOSTS	HOSTS file
	Удалить URL из конфигурации браузера	Firefox configuration, Chromium configuration
Cure	Вылечить объект	Signature detections
Run	Запустить задание	Scheduled tasks
Set Value	Задать значение	Registry

Действия представляют собой команды, которые войдут в лечащую утилиту FixIt! (см. раздел Команды утилиты).

Выбранные для каждого объекта действия отображаются на вкладке Выбранные действия.

14.2. Новый фильтр

На вкладке **Новый фильтр** вы можете создать новый фильтр, в том числе на основе готового. Кроме того, на этой вкладке вы можете:

- редактировать фильтры;
- удалять фильтры;
- создавать группы фильтров;

- выполнять поисковые запросы с готовыми фильтрами или вручную ввести запрос и поля запроса;
- применять действия к угрозам.

Структура фильтра

Фильтр состоит из следующих компонентов:

- **Запрос.** По нему выполняется поиск по данным. Запрос состоит из аргументов (категорий объектов, по которым выполняется поиск) и их значений (то есть параметров конкретных объектов внутри категории).
- **Поля.** Определяет, какие данные будут выведены в результате запроса. В одном фильтре может быть несколько полей, которые указываются через запятую.

Поле **Запрос** можно также использовать для обычного поиска, например по названию файла, который вы уже определили как вредоносный. Единственным отличием будет необходимость указать поля, то есть графы таблицы с данными о найденных объектах, в которой будут выведены результаты поиска.

Например, при указании поля `path` в результатах будет выведен путь к найденным файлам, поле `state` выведет состояние найденных объектов, а поле `hash.sha256` — отпечатки SHA256.

FixIt! позволяет выполнять поиск по частичному совпадению в имени файла. Для этого используются символы-джокеры «*» и «?». Знак звездочки «*» означает любое число любых символов, в том числе отсутствие символа, а вопросительный знак «?» означает любой одиночный символ.

Например, поиск по запросу `files*` выведет файлы с именем `files`, `files111`, `files systems`, `files_more_worlds` и т. д.

Поиск по запросу `files?` выведет файлы с именем `files1`, `filess`, `files_`, но файл с именем `files` не выведет.

Более подробную информацию о запросах читайте в разделе Составление запросов.

Доступ к фильтрам

Вы можете настроить доступ к фильтру, сделав его видимым для других пользователей сервиса или только для вас. Возможны следующие варианты доступа:

- **Для всех.** Опция доступна только для администраторов. Фильтр будет виден всем пользователям сервиса.
- **Для этого пространства.** Опция доступна только для менеджеров и пользователей. Фильтр будет виден всем участникам пространства.

- **Для меня.** Опция доступна всем пользователям сервиса. Фильтр будет виден только пользователю, создавшему фильтр.
- **Для текущей задачи.** Опция доступна всем пользователям сервиса. Фильтр будет виден всем пользователям, работающим с этой задачей.

Создание фильтра

Создать фильтр может любой пользователь сервиса.

Чтобы создать фильтр

1. На вкладке **Новый фильтр** заполните поле **Запрос**.

   Чтобы добавить новую строку в поле **Запрос**, используйте комбинацию клавиш CTRL + ENTER.

2. Заполните **Поля**.
3. Нажмите **Сохранить как новый фильтр**. Появится окно **Сохранение фильтра**.
4. В поле **Имя** введите имя фильтра.
5. (Необязательно) Добавьте фильтр в избранное, установив переключатель **В избранное**.
6. (Необязательно) В поле **Описание** добавьте описание для фильтра.
7. В поле **Доступен** укажите, кому будет доступен фильтр.
8. (Необязательно) Выберите группу или создайте новую, нажав **Новая группа** и заполнив необходимые поля.
9. Нажмите **Сохранить**.

Когда фильтр будет создан, в левом нижнем углу экрана появится соответствующее уведомление.

После сохранения фильтр необратимо изменится для всех пользователей сервиса.

Редактирование и удаление фильтра

Редактировать и удалять фильтры категории **Для всех** могут только администраторы. Редактировать и удалять фильтры категорий **Для пространства**, **Для задачи** и **Для меня** может любой пользователь сервиса.

Чтобы редактировать фильтр

1. На вкладке **Новый фильтр** нажмите **Добавить**.

2. Выберите фильтр, который хотите изменить, и нажмите **Добавить**.
3. Измените параметры фильтра.
4. Если вы хотите сохранить изменения в имеющемся фильтре:

- Нажмите **Сохранить изменения** и подтвердите действие во всплывающем окне.

> После сохранения вы необратимо измените фильтр для всех пользователь сервиса, которым доступен этот фильтр.

Если вы хотите сохранить измененный фильтр как новый:

- Нажмите **Сохранить как новый фильтр**.

В процессе редактирования фильтра вы можете сбросить несохраненные изменения, нажав кнопку **Сбросить**.

После сохранения изменений созданным фильтром можно пользоваться как готовым.

Чтобы удалить фильтр

1. На вкладке **Новый фильтр** нажмите **Добавить**.
2. Выберите фильтр, который хотите удалить, и нажмите **Добавить**.
3. Нажмите **Удалить**.
4. Подтвердите удаление во всплывающем окне.

> Если вы удалили фильтр по ошибке, в течение нескольких секунд вы можете отменить это действие, нажав **Отменить** во всплывающем уведомлении в верхней части окна.

Быстрое применение фильтра

Вы можете заполнить **Запрос** и **Поля** на вкладке **Новый фильтр**, а затем сразу, не сохраняя фильтр, применить его.

Чтобы быстро применить фильтр (без сохранения)

1. На вкладке **Новый фильтр** заполните поля **Запрос** и **Поля**.
2. Нажмите **Применить**.

> Чтобы применить фильтр, вы также можете нажать клавишу ENTER прямо в поле **Запрос** или **Поля**.

14.2.1. Составление запросов

Запрос — это первая часть фильтра FixIt!, которая отвечает за выбор объектов, данные по которым вы хотите просмотреть.

Вторая часть, **Поля**, отвечает за то, какие именно данные о выбранных объектах вы хотите вывести.

В этом разделе описано, как составлять *запросы*.

Структура и синтаксис запросов

Запрос состоит из:

- аргументов (категорий объектов, по которым выполняется поиск),
- значений (параметров конкретных объектов внутри категории).

В одном запросе можно задать поиск сразу по нескольким условиям, объединив их при помощи логических операторов. Для группировки условий используются круглые скобки `(...)`.

Пример:

```
category_name: "files" AND arkstatus.file: (ts_malware OR ts_suspicious)
```

По этому запросу вы найдете все объекты типа «файл», у которых значение `arkstatus.file` соответствует значениям, которые присваиваются как вредоносным, так и подозрительным файлам.

Операторы запросов

Основные операторы, которые используются для объединения условий в запросе, — *AND*, *OR* и *AND NOT*.

- Чтобы найти элементы, для которых одновременно выполняются *все заданные условия*, используйте оператор AND. Вместо него можно использовать символ (+) перед элементом.
- Чтобы найти элементы, для которых выполняются *любые из заданных условий*, используйте оператор OR.
- Чтобы найти элементы, для которых *не выполняются* заданные после этого оператора условия, используйте оператор AND NOT. Вместо него можно использовать символ (–) перед элементом.

Кроме того, в запросах используются символьные операторы.

В таблице ниже приведены символьные операторы, которые можно использовать при составлении запросов, и их значения.

Оператор	Значение
.	Заменяет любой символ. Пример: `ab.` будет соответствовать результатам `aba`, `abb`, `abz` и т. д.
?	Относится к предыдущему символу, делая его опциональным в поиске. Пример: `abc?` будет соответствовать результатам `ab` и `abc`.
+	Повторяет предыдущий символ минимум один раз. Пример: `ab+` будет соответствовать результатам `ab`, `abb`, `abbb` и т. д.
*	Повторяет предыдущий символ произвольное число раз и делает его опциональным. Пример: `ab*` будет соответствовать результатам `a`, `ab`, `abb`, `abbb` и т. д.
{...}	В фигурных скобках указывается минимальное и максимальное число повторов предыдущего символа. Пример: • `a{2}` будет соответствовать результату `aa` • `a{2,4}` будет соответствовать результатам `aa`, `aaa` и `aaaa` • `a{2,}` будет соответствовать результатам со значением `a`, повторенным два раза или более.
|	Соответствует оператору OR. В результатах будут выведены совпадения как по левой, так и по правой части выражения, разделенного этим символом. Пример: `abc|xyz` будет соответствовать результатам `abc` и `xyz`.
(...)	Объединяет значения в группы. Такая группа будет трактоваться как одно значение. Пример: `abc(def)?` будет соответствовать результатам `abc` и `abcdef`, но не будет соответствовать `abcd`.
[...]	Выводит результаты, соответствующие одному из значений в скобках. Пример: `[abc]` будет соответствовать результатам `a`, `b`, `c` При добавлении знака дефиса (`-`) между значениями в квадратных скобках в результатах выводится диапазон, если дефис не стоит в начале и если он не экранирован с помощью знака `\`. Пример: • `[a-c]` будет соответствовать результатам `a`, `b` или `c` • `[-abc]` будет соответствовать результатам `-`, `a`, `b` или `c` (дефис будет считаться первым значением)

	• `[abc\-]` будет соответствовать результатам `a`, `b`, `c` или – (дефис экранирован)
^	Знак ^ перед значением в квадратных скобках означает, что значение или диапазон значений будут исключены из результатов. Пример: • `[^abc]` будет соответствовать всем результатам, кроме `a`, `b` или `c` • `[^a-c]` будет соответствовать всем результатам, кроме `a`, `b` или `c` • `[^-abc]` будет соответствовать всем результатам, кроме `-`, `a`, `b` или `c` • `[^abc\-]` будет соответствовать всем результатам, кроме `a`, `b`, `c` или `-`.

Диапазоны значений

Если требуется зайти по запросу объекты с типом данных «дата», «число» или «строка», для них можно указывать диапазоны значений.

- Если крайние значения входят в нужный диапазон, используются квадратные скобки `[...]`: `[min TO max]`
- Если крайние значения не входят в диапазон, используются фигурные скобки `{...}`: `{min TO max}`
- Если крайнее значение входит в диапазон только с одной стороны: скобки комбинируются: `[min TO max}`
- Если диапазон ограничен только с одной стороны, используется символ `*`: `[min TO *]`

Для обозначения диапазонов также используется упрощенный синтаксис.

Для диапазонов, ограниченных с одной стороны:

- `size:>10`
- `size:>=10`
- `size:<10`
- `size:<=10`

Для диапазонов, ограниченных с обеих сторон, в упрощенном синтаксисе применяется группировка условий:

- `size:(>=10 AND <20)`
- `size:(+>=10 +<20)`

14.3. Выбранные действия

В разделе **Выбранные действия** отображаются действия, которые были выбраны для объектов на вкладке **Готовые фильтры**. Выбранные действия будут применены к объектам лечащей утилитой FixIt!. Набор доступных действий зависит от характеристик объекта.

Раздел **Выбранные действия** позволяет:

- просмотреть выбранные действия,
- изменить выбранные действия,
- перейти к созданию утилиты FixIt! с выбранными действиями.

Объекты, для которых были выбраны действия, представлены в разделе **Выбранные действия** в выпадающих списках, соответствующих типу объекта. Для каждого типа объекта отображается таблица с параметрами объектов указанного типа. В первом столбце таблицы указано действие, выбранное для каждого объекта. Данные таблицы можно упорядочить, нажав значок ▲▼ в нужном столбце таблицы.

Чтобы обновить список объектов, для которых были выбраны действия

- Нажмите кнопку **Обновить**.

Чтобы изменить выбранное действие

1. Нажмите действие, выбранное для объекта.
2. Выберите новое действие в выпадающем списке.

Чтобы собрать утилиту с выбранными действиями

- Нажмите кнопку **Создать** на вкладке **Выбранные действия**. Откроется вкладка Утилита FixIt!.

15. Утилита FixIt!

Утилита FixIt! — это исполняемый файл (*.exe), который собирает данные о системе проверяемого компьютера и формирует подробный отчет. Утилита исследует:

- установленные программы и обновления;
- запущенные и запускаемые процессы;
- подозрительные записи в реестре и их связи с другими объектами;
- установленные драйверы и расширения браузеров;
- модули, загруженные в процессы;
- системные журналы;
- разделы дисков.

Проанализировав отчет, вы можете добавить в утилиту нужные вам команды лечения. Такая утилита, помимо сбора данных, устранит проблемы и обезвредит обнаруженные угрозы на проверяемом компьютере.

Если утилита только собирает данные, она называется *анализирующей*, а если может устранять проблемы, — *лечащей*.

15.1. Как создать утилиту FixIt!

- Если в нужной задаче нет загруженных отчетов:
  1. Зайдите в задачу.
  2. Нажмите кнопку **Создать утилиту FixIt!**.
  3. (Необязательно) Измените настройки утилиты. Для этого в правом нижнем углу панели **Утилита FixIt!** нажмите **Настройки** и задайте нужные настройки.
  4. (Необязательно) На панели **Утилита FixIt!** введите команды, которые вы хотите дополнительно включить в утилиту.
  5. Нажмите **Создать утилиту FixIt!**.
- Если в нужной задаче уже есть загруженные отчеты:
  1. Зайдите в задачу.
  2. Откройте любой отчет из списка.
  3. На боковой панели слева выберите **Утилита FixIt!**.
  4. (Необязательно) Измените настройки утилиты. Для этого в правом нижнем углу панели **Утилита FixIt!** нажмите **Настройки** и задайте нужные настройки.
  5. (Необязательно) На панели **Утилита FixIt!** введите команды, которые вы хотите дополнительно включить в утилиту.
  6. Нажмите **Создать утилиту FixIt!**.

Когда утилита будет создана, на экране появится окно, в котором вы сможете выбрать, как отправить утилиту владельцу проверяемого компьютера:

- Если вы хотите сохранить утилиту на своем компьютере и отправить сохраненный файл владельцу проверяемого компьютера, нажмите **Скачать утилиту FixIt!** и отправьте владельцу скачанный файл.
- Если вы хотите, чтобы владелец проверяемого компьютера скачал утилиту самостоятельно, скопируйте ссылку, нажав значок , и отправьте ее владельцу компьютера.

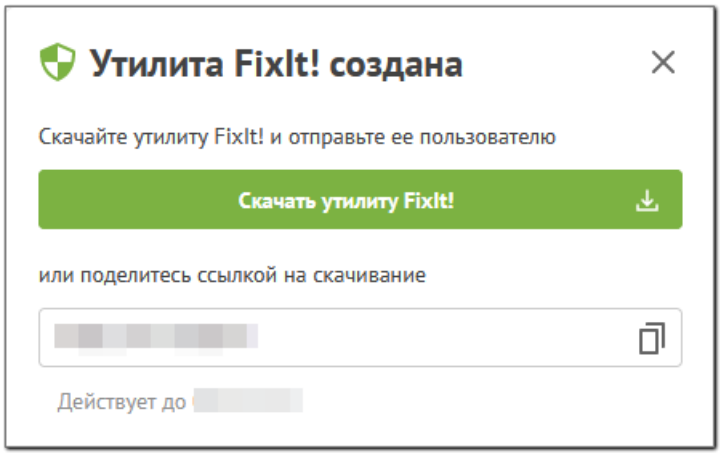

Рисунок 12. Утилита FixIt! создана

15.2. Настройки утилиты

Вы можете задать настройки при создании утилиты FixIt!. Эти настройки сохраняются для всех последующих лечащих утилит этой задачи. Чтобы изменить настройки, создайте утилиту FixIt! еще раз.

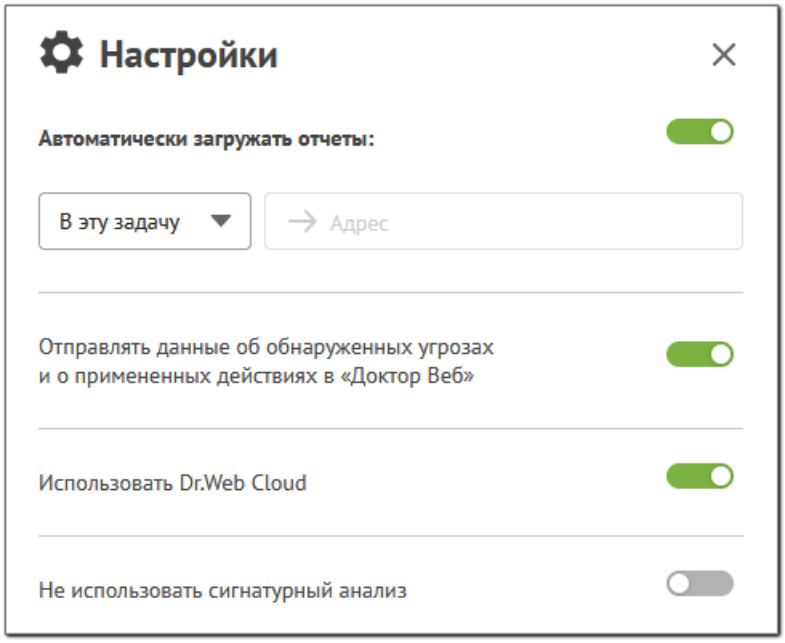

Рисунок 13. Настройки утилиты FixIt!

В следующей таблице приведено описание всех настроек утилиты FixIt!.

Настройка	Описание
Автоматически загружать отчеты в эту задачу	После проверки системы загружать отчеты в задачу автоматически. Для этого на проверяемом компьютере требуется активное интернет-соединение. Если отчет не загрузится автоматически, загрузите его вручную. Отчет сохраняется локально на проверяемом компьютере. Ссылка на файл доступна в окне утилиты FixIt! после окончания проверки.
Автоматически загружать отчеты на URL	После проверки системы загружать отчеты автоматически на указанный URL. Для этого на проверяемом компьютере требуется интернет-соединение. Если отчет не загрузится автоматически, загрузите его вручную. Отчет сохраняется локально на проверяемом компьютере. Ссылка на файл доступна в окне утилиты FixIt! после окончания проверки.
Отправлять данные об обнаруженных угрозах и о примененных действиях в «Доктор Веб»	Отправлять данные о найденных угрозах и примененных к ним действиях для улучшения качества продуктов компании «Доктор Веб». Личные данные не отправляются.
Использовать Dr.Web Cloud	Использовать Dr.Web Cloud во время проверки компьютера, чтобы улучшить обнаружение угроз. Этот облачный сервис хранит информацию об угрозах, записи о которых пока отсутствуют в антивирусных базах Dr.Web, и позволяет находить новейшие угрозы без обновления антивирусных баз на устройстве.
Не использовать сигнатурный анализ	Не использовать сканирующий сервис Dr.Web Scanning Engine и антивирусные базы Dr.Web при проверке системы. Настройка позволяет уменьшить размер утилиты. Рекомендуется только в том случае, если на проверяемом компьютере уже установлен антивирусный продукт Dr.Web.

15.3. Команды утилиты

Вы можете вручную добавить в утилиту FixIt! нужные вам команды сбора информации и лечения.

Синтаксис

Каждая команда указывается с новой строки и имеет следующий формат:

```
<Название команды> <Опции, аргументы или значения, разделенные пробелами>
```

Значения аргументов могут быть строковыми, бинарными и числовыми. Если не указано иное, значение считывается как строка.

Тип	Описание	Примеры
Строковый	Если значение начинается с двойной кавычки (`"`), оно считывается до такой же закрывающей кавычки. При этом экранированные кавычки (`\"`) преобразуются в обычные и считываются в составе строки. Иначе значение считывается до пробела, комментария, конца строки или конца файла.	`fs-remove c:\con` `fs-remove "c:\con 2"`
Бинарный	Значения считываются парами HEX-цифр.	`0B8E` (2 байта)
Числовой	Значения являются беззнаковыми и пишутся в десятичном или шестнадцатеричном формате.	`15` `0xFE`

Комментарии к командам начинаются символом #.

Валидация кода

Ошибки синтаксиса подсвечиваются в поле ввода команд и выводятся в нижней панели поля ввода. Нажмите панель > **Ошибки**, чтобы просмотреть список обнаруженных валидатором ошибок и их описания. Для создания утилиты FixIt! необходимо устранить все ошибки.

Список команд

Скрипт с командами выполняется последовательно в три этапа:

1. Антируткитный сканер. На этом этапе команды выполняются в произвольном порядке.
2. Скриптовые команды. На этом этапе команды выполняются в том порядке, в котором указаны.
3. Сбор информации. На этом этапе команды выполняются в произвольном порядке.

15.3.1. Команды сбора информации

Команды сбора информации используются, чтобы получить информацию об объектах, которые не попали в отчет при штатном запуске утилиты. Для сбора информации о конкретном объекте добавьте команду сбора информации в скрипт вручную. Для этого введите нужные команды в области команд на панели **Утилита FixIt!**.

Ниже указаны доступные команды. Чтобы просмотреть список доступных команд в сервисе, нажмите кнопку {i} **Команды** на вкладке **Утилита FixIt!**.

Команда	Описание
`inspect-fs [-r] [-p] <Путь>`	Собрать информацию о файле или каталоге. Если указана опция `-r`, то информация будет собрана об указанном каталоге и рекурсивно о каждом файле и подкаталоге. Если указана опция `-p`, то для получения списка файлов будет по возможности использоваться парсер файловой системы (FAT/NTFS). Применяется только для каталогов. В каталог `ARTEFACTS` попадают файлы. Пример: `inspect-fs -r "C:\Malware"` Поддерживаются маски при задании имени файла. Маска задает общую часть имени файла. При этом: • символ «*» заменяет любую, возможно, пустую, последовательность символов; • символ «?» заменяет любой, но только один символ; • остальные символы маски ничего не заменяют и означают, что на этом месте в имени должен находиться именно этот символ. Примеры: • отчет*.pdf – маска, задающая все PDF-документы, название которых начинается с подстроки «отчет», например, файлы отчет-февраль.pdf, отчет121209.pdf и т. д.; • *.exe – маска, задающая все файлы с расширением EXE, например, setup.exe, iTunes.exe и т. д.; • photo????09.jpg – маска, задающая все файлы изображений формата JPG, название которых начинается с подстроки «photo» и заканчивается подстрокой «09», при этом между двумя этими подстроками в названии файла стоит ровно четыре произвольных

Команда	Описание
	символа, например, photo121209.jpg, photomama09.jpg или photo----09.jpg.
`inspect-reg <SID> <Путь к ключу>`	Собрать информацию о ключе реестра. Допустимые значения <*SID*>: `.DEFAULT`, `HKLM`, `HKCU` и `HKU`, а также значения, начинающиеся с последовательности символов `S-1-5`. Пример: `inspect-reg HKLM "SOFTWARE\Malware"`
`inspect-proc --pid <PID> /--imagename <Имя> / --imagepath <Путь> / --cmdline <Командная строка>`	Собрать информацию о процессах. В каталог `ARTEFACTS` попадают дампы процессов. Пример: `inspect-proc --imagename win32calc.exe`
`inspect-disk <Disk ID> <Сектор> <Количество>`	Собрать информацию о секторах диска. В каталог `ARTEFACTS` попадает дамп секторов. Пример: `inspect-disk 0 10 2`
`inspect-drv --imagebase <База образа> / --imagesize <Размер образа> / --imagename <Имя> / --imagepath <Путь>`	Собрать информацию о драйверах с указанными базами образов, размером, именем или путем к файлу. В каталог `ARTEFACTS` попадают дампы драйверов. Пример: `inspect-drv --imagebase 0xfffff8064e540000`

15.3.2. Команды лечения

Получив отчет о проверяемом компьютере, вы можете проанализировать полученные данные (см. раздел Поиск и анализ) с помощью фильтров, применить действия к выбранным угрозам и создать лечащую утилиту FixIt! с заданным скриптом лечения.

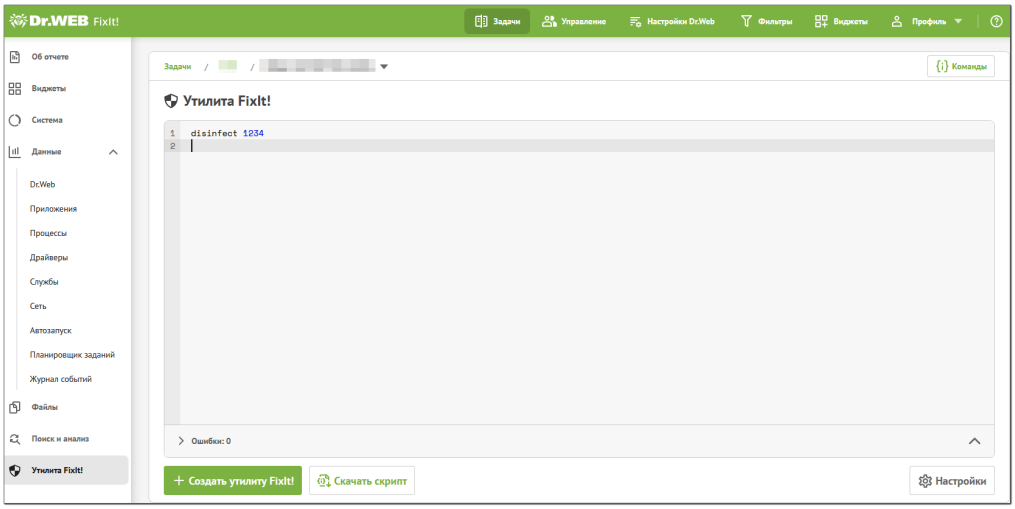

Рисунок 14. Создание лечащей утилиты FixIt!

При необходимости вы можете добавить команды лечения в скрипт вручную. Команды соответствуют типу объекта.

Ниже указаны все доступные команды лечения. Вы также можете просмотреть список доступных команд прямо в сервисе. Для этого на вкладке **Утилита FixIt!** нажмите кнопку {i} **Команды**.

Антируткитный сканер

Команда	Описание
`disinfect <ID>`	Вылечить системный объект с указанным внутренним идентификатором. Обычно применяется к объектам типа Несигнатурные детекты. Идентификатор присваивается в процессе сборки отчета. Пример: `disinfect "10b2e828339cae479b1e5310b5980b717b7bcc57"`
`disinfect-reg <ID>`	Вылечить элемент автозагрузки реестра с указанным внутренним идентификатором. Применяется к объектам типа Запланированные задания. Идентификатор присваивается в процессе сборки отчета. Пример: `disinfect-reg "629387a5dbc86d60842f12af5c43ffa5816140cc"`

Команда	Описание
`ark-disinfect --imagepath <Путь> / --sha256 <Значение>`	Выполнить комплексное обезвреживание активных объектов, найденных по указанному признаку. Если задан `Путь`, то будет удален файл по указанному пути, а также завершены соответствующие процессы, если файл исполняемый. Если указано значение `SHA256`, то будет проведен поиск по файлам среди активных процессов. Соответствующие найденные файлы будут удалены, а сами процессы завершены. Пример: `ark-disinfect --sha256 "71b969b079beba0db952399b918cdb6781aa5b5a1c3295129df92a0dd0fa457f"`

Скриптовые команды

Команда	Описание
Сигнатурные детекты	
`cure-file <Путь>`	Вылечить файл, в котором обнаружена сигнатура угрозы. Действия (удаление, лечение содержимого с заменой, дополнительные действия в системе) определяются сигнатурой, обнаруженной в файле. При лечении удалением учитывается расположение файла, активность в системе и др. При необходимости производятся дополнительные действия: отложенное удаление, очистка элементов автозагрузки, блокировка пути до перезагрузки и др. Если файл окажется чист при вызове команды, ничего не произойдет. Пример: `cure-file C:\Windows\System32\malware.exe`
Файловая система	
`fs-move <Источник> <Назначение>`	Переместить или переименовать файл или каталог.

Команда	Описание
	Если `Назначение` — существующий каталог, то `Источник` перемещается в `Назначение`. Иначе `Источник` переименовывается в `Назначение`. Пример: `fs-move c:\con c:\lpt1`
`fs-remove` <*Путь*>	Удалить файл или каталог по указанному пути. В конце отчета будут указаны не удаленные ссылки на объект и связи между этим объектом и прочими, которые останутся в системе. Пример: `fs-remove c:\con`
`fs-reset-acl [-r]` <*Путь*>	Установить родительский ACL для файла или каталога. Если указана опция `-r`, ACL назначается рекурсивно для каждого файла и подкаталога. Если в процессе рекурсивного обхода не удалось назначить родительский ACL для определенного каталога, для этого каталога прекращается обход в глубину во избежание установки некорректного ACL на дочерние элементы. Пример: `fs-reset-acl -r c:\test1\test2`
`fs-clear-ads` <*Путь*>	Удалить все ADS файла или каталога. Пример: `fs-clear-ads C:\windows\explorer.exe`
Реестр	
`reg-remove` <*SID*> <*Путь к ключу*> [<*Значение*>]	Удалить значение или ключ. <*SID*> — профиль реестра. Допустимые значения <*SID*>: `.DEFAULT`, `HKLM`, `HKCU` и `HKU`, а также значения, начинающиеся с последовательности символов `S-1-5`.

Команда	Описание

	В конце отчета будут указаны не удаленные ссылки на объект и связи между этим объектом и прочими, которые останутся в системе.
	Примеры:
	`reg-remove HKLM SOFTWARE\Test`
	`reg-remove HKLM SOFTWARE\Test Value`

`reg-set-value [-f]` *<SID> <Путь к ключу> <Имя значения> <Тип> <Данные значения>*	Задать значение для заданного ключа. *<SID>* — профиль реестра.
	Допустимые значения *<SID>*: `.DEFAULT`, `HKLM`, `HKCU` и `HKU`, а также значения, начинающиеся с последовательности символов `S-1-5`.
	Если указана опция `-f`, создаются родительские ключи (если они отсутствовали), а ключ перезаписывается с новым типом.
	• Значения типов REG_SZ, REG_EXPAND_SZ задаются в строковом формате.
	• Значения типов REG_BINARY, REG_MULTI_SZ задаются в бинарном формате.
	• Значения типов REG_DWORD, REG_QWORD задаются в числовом формате.
	Примеры:
	`reg-set-value -f HKLM SOFTWARE\Test TestSZ REG_SZ "Test"`
	`reg-set-value -f HKLM SOFTWARE\Test TestBINARY REG_BINARY "530053004400500053005200 5600"`
	`reg-set-value -f HKLM SOFTWARE\Test TestDWORD REG_DWORD 0x1`

`reg-reset-acl [-r]` *<Путь к ключу>*	Установить родительский ACL на ключ. Если указана опция `-r`, ACL сбрасывается рекурсивно для каждого подраздела. Если в процессе рекурсивного обхода не удалось назначить родительский ACL для определенного ключа, для этого ключа прекращается обход в глубину, чтобы избежать установки некорректного ACL на дочерние элементы.

Команда	Описание
	Пример: `reg-reset-acl -r HKLM SOFTWARE\Test`
Процессы	

`proc-dump [-f] --pid <PID> / --imagename <Имя> / --imagepath <Путь> / --cmdline <Командная строка>`	Формировать сокращенный или полный (`-f`) дамп памяти для процесса, соответствующего заданным критериям; дамп создается во временном каталоге и записывается в артефакты на этапе сбора отчета.
	Примеры:
	`proc-dump --pid 4123`
	`proc-dump -f --imagepath C:\tools\procexp.exe`
	`proc-dump -f --cmdline C:\test\procexp64.exe`

`proc-execute [-w] <Путь> [<Аргументы>]`	Запустить процесс по указанному пути с указанными аргументами. В пути могут использоваться системные переменные. Если задан флаг `-w`, то команда будет ждать, пока процесс не завершится.
	Пример:
	`proc-execute c:\Windows\System32\win32calc.exe`
	Примеры с системной переменной:
	`proc-execute %TEMP%\sample.exe`
	`proc-execute \\?\%windir%\notepad.exe`

`proc-kill --pid <PID> / --imagename <Имя> / --imagepath <Путь> / --cmdline <Командная строка>`	Завершить указанные процессы. Пример: `proc-kill --imagename win32calc.exe`
`proc-suspend --pid <PID> / --imagename <Имя> / --imagepath <Путь> / --cmdline <Командная строка>`	Заморозить указанные процессы.

Команда	Описание
	Пример: `proc-suspend --imagename win32calc.exe`
Службы	
`svc-start <Имя>`	Запустить службу с указанным именем. Пример: `svc-start TestService`
`svc-stop <Имя>`	Остановить службу с указанным именем. Пример: `svc-stop TestService`
`svc-delete <Имя>`	Удалить службу с указанным именем. В конец отчета добавляется информация о не удаленных файлах, связанных со службой. Пример: `svc-delete TestService`
`svc-control <Имя> <Управляющий код>`	Отправить управляющий код службе с указанным именем. Пример: `svc-control TestService 3`
Запланированные задачи	
`task-run <Путь>`	Запустить задание с указанным именем. Пример: `task-run \Microsoft\Windows\TestTask`
`task-delete <Путь>`	Удалить задание с указанным именем. В конец отчета добавляется информация о необработанных связях, указывающих на файлы, на которые ссылается объект.

Команда	Описание
	Пример: `task-delete \Microsoft\Windows\TestTask`
Многоуровневые поставщики услуг	
`lsp-delete <GUID>`	Удалить зарегистрированные провайдеры с указанным в реестре `GUID`. Пример: `lsp-delete {f9eab0c0-26d4-11d0-bbbf-00aa006c34e4}`
Поставщики пространства имен	
`nsp-delete <GUID>`	Удалить зарегистрированные провайдеры с указанным в реестре `GUID`. Пример: `nsp-delete {6642243a-3ba8-4aa6-baa5-2e0bd71fdd83}`
Поставщики WMI	
`wmi-delete-eventconsumer <Пространство имен> <Класс> <Имя>`	Удалить объект WMI EventConsumer из указанного пространства имен. Пример: `wmi-delete-eventconsumer ROOT\subscription CommandLineEventConsumer CommandLineTemplate`
`wmi-query <Пространство имен> <Запрос> <Значения>`	Выполнить запрос query к WMI и вывести в лог значения, указанные в values. Пример: `wmi-query root\cimv2 SELECT * FROM Win32_Process Name,ProcessId,CommandLine,ThreadCount,WorkingSetSize`
Файл HOSTS	
`hosts-clear <Путь> <Строка> [<Строки>]`	Закомментировать ("#" + line) указанные строки из файла HOSTS. Нумерация с единицы.

Команда	Описание
	Пример: `hosts-clear c:\Windows\System32\drivers\etc\hosts 44 45 46`
`hosts-default <Путь>`	Восстановить стандартный для системы файл HOSTS. Пример: `hosts-default c:\Windows\System32\drivers\etc\hosts`
`hosts-cure <Путь>`	Проверить все записи файла HOSTS и закомментировать все записи, IP-адреса в которых определятся как вредоносные. При этом в файл добавляется строка `# cured by Dr.Web`. Пример: `hosts-cure c:\Windows\System32\drivers\etc\hosts`
Расширения и конфигурация браузеров	

`chromium-remove-ext <Браузер> <SID> <Профиль> <ID расширения>`	Удалить расширение браузера для указанного профиля.
	Допустимые значения <*SID*>: `.DEFAULT`, `HKLM`, `HKCU` и `HKU`, а также значения, начинающиеся с последовательности символов `S-1-5`.
	Примеры:
	`chromium-remove-ext Chrome S-1-5-21-120241661-1916511805-682617159-1001 default geadmilgigoffmcnlfdlpihockonlopf`
	`chromium-remove-ext Opera S-1-5-21-120241661-1916511805-682617159-1001 "" geadmilgigoffmcnlfdlpihockonlopf`

`firefox-remove-ext <Браузер> <SID> <Профиль> <ID расширения>`	Удалить расширение браузера для указанного профиля. Допустимые значения <*SID*>: `.DEFAULT`, `HKLM`, `HKCU` и `HKU`, а также значения, начинающиеся с последовательности символов `S-1-5`.

Команда	Описание
	Пример: `firefox-remove-ext Firefox S-1-5-21-120241661-1916511805-682617159-1001 default default-theme@mozilla.org`
`chromium-clear` *<Браузер>* *<SID>* *<Профиль>* *<URL>*	Удалить URL из конфигурации браузера для указанного профиля. Допустимые значения *<SID>*: `.DEFAULT`, `HKLM`, `HKCU` и `HKU`, а также значения, начинающиеся с последовательности символов `S-1-5`. Пример: `chromium-clear Chrome S-1-5-21-120241661-1916511805-682617159-1001 Default malware.com`
`firefox-clear` *<Браузер>* *<SID>* *<Профиль>* *<URL>*	Удалить URL из конфигурации браузера для указанного профиля. Допустимые значения *<SID>*: `.DEFAULT`, `HKLM`, `HKCU` и `HKU`, а также значения, начинающиеся с последовательности символов `S-1-5`. Пример: `firefox-clear Firefox S-1-5-21-120241661-1916511805-682617159-1001 default malware.com`
Dr.Web	
`drweb-remove`	Удалить из системы ПО Dr.Web и/или его следы. Пример: `drweb-remove`
Пользователи	
`user-delete` *<Имя пользователя>*	Удалить указанного пользователя на станции.
Система	
`reboot [-f]`	Перезагрузить систему, показав системное диалоговое окно с 1-минутным тайм-аутом. Команда прерывает дальнейший сбор отчета.

Команда	Описание
`shutdown [-f]`	Завершить работу системы, показав системное диалоговое окно с 1-минутным тайм-аутом. Команда прерывает дальнейший сбор отчета.

15.4. Скрипт

Вы можете скачать последовательность команд, отображающихся в области команд на панели **Утилита FixIt!**, в виде файла CFG, *скрипта*, и отправить этот скрипт пользователю вместо утилиты. Это удобно, к примеру, если вы ранее уже отправили пользователю утилиту и теперь хотите повторить проверку, дополнив утилиту новыми командами (например, командами лечения).

Чтобы отправить скрипт пользователю

1. Зайдите в задачу.
2. Откройте любой отчет из списка.
3. На боковой панели слева выберите **Утилита FixIt!**.
4. Введите команды, которые нужно включить в скрипт, на панели **Утилита FixIt!**.
5. Нажмите **Скачать скрипт**.

На экране появится следующее окно, в котором вы сможете выбрать, как отправить скрипт владельцу проверяемого компьютера.

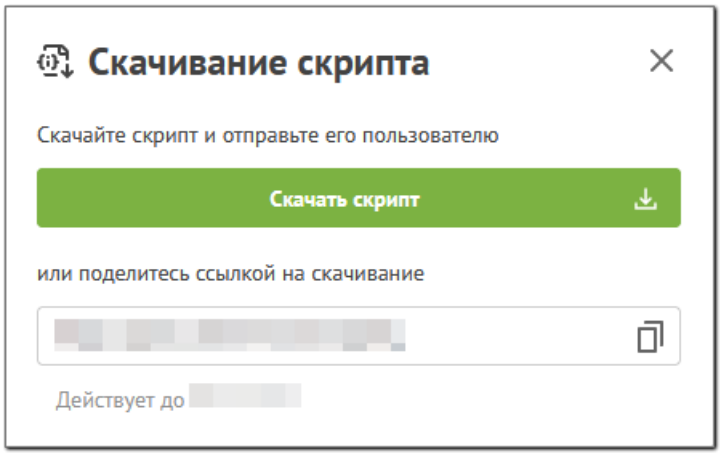

Рисунок 15. Скачивание скрипта

- Если вы хотите сохранить скрипт на своем компьютере и отправить сохраненный файл владельцу проверяемого компьютера, нажмите **Скачать скрипт** и отправьте владельцу скачанный файл.
- Если вы хотите, чтобы владелец проверяемого компьютера скачал скрипт самостоятельно, скопируйте ссылку, нажав значок , и отправьте его владельцу компьютера.

15.5. Как проверить компьютер утилитой FixIt!

Этот раздел предназначен для пользователей проверяемых компьютеров.

Утилита FixIt! не требует установки. Чтобы начать работу, просто запустите исполняемый файл утилиты на проверяемом компьютере.

Чтобы проверить компьютер утилитой FixIt!

1. Запустите исполняемый файл утилиты FixIt! на своем компьютере. Откроется начальный экран утилиты.
2. (Необязательно) Измените заданные по умолчанию параметры отчета и путь к каталогу, в котором будет сохранен отчет.
3. Нажмите **Начать сканирование**. Утилита соберет информацию о состоянии вашего компьютера.

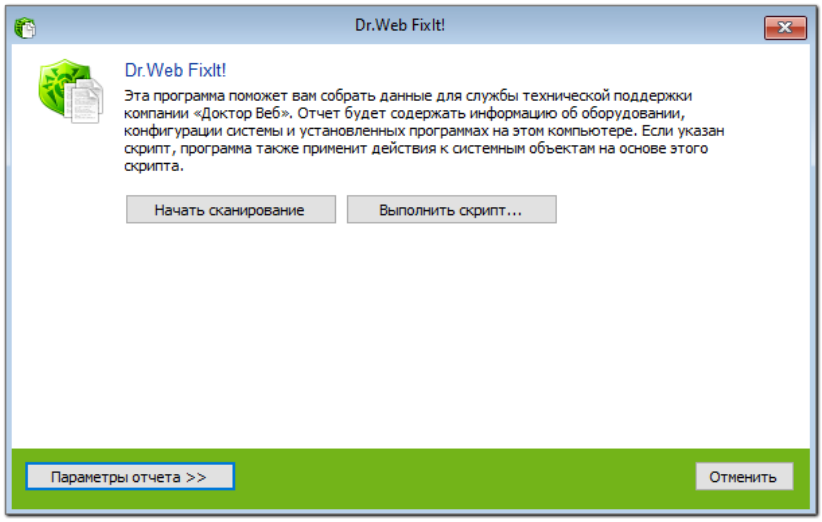

Рисунок 16. Начальный экран утилиты FixIt!

Если нужно прервать сбор данных, нажмите **Отменить**. Прерванную операцию продолжить нельзя, утилиту FixIt! потребуется запустить заново.

По окончании проверки утилита FixIt! создаст ZIP-архив с отчетом в папке, которая была указана в параметрах отчета. По умолчанию это папка `C:\Users\<Пользователь>\Doctor Web`. В ту же папку будет сохранен файл с расширением `.zip_password.txt`, представляющий собой текстовый документ с паролем от ZIP-архива. В окне утилиты FixIt! отобразится ссылка на ZIP-архив с отчетом.

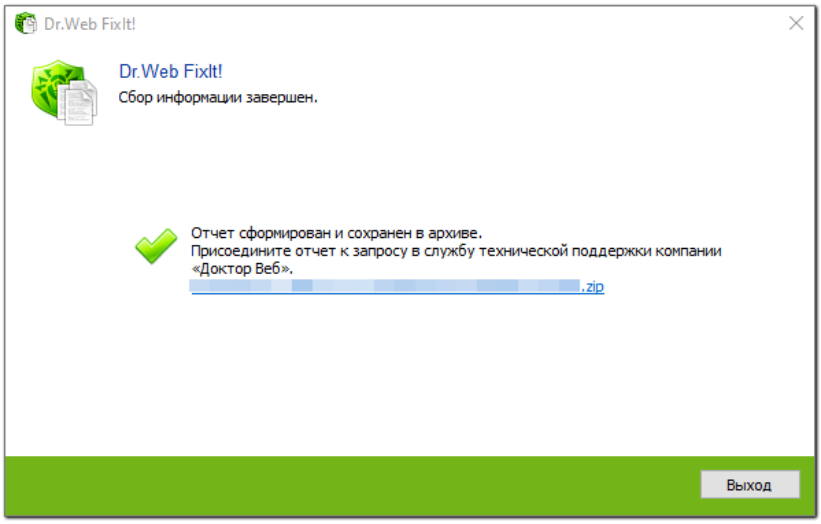

Рисунок 17. Ссылка на созданный отчет

Параметры отчета

Прежде чем запустить утилиту FixIt!, вы можете указать, какие данные хотите включить в отчет. Для этого запустите исполняемый файл утилиты FixIt! на проверяемом компьютере, в нижней части главного экрана утилиты нажмите **Параметры отчета** и установите флажки напротив нужных вам категорий данных.

Кроме того, вы можете указать путь к каталогу, в котором будет сохранен ZIP-архив с отчетом. Для этого нажмите **Обзор**, выберите нужный каталог и нажмите **OK**.

Скрипт

Если вы получили от оператора скрипт, запустите его на выполнение вместе с утилитой FixIt!.

Чтобы запустить скрипт на выполнение вместе с утилитой FixIt!

1. Запустите исполняемый файл утилиты FixIt! на своем компьютере. Откроется начальный экран утилиты.
2. (Необязательно) Измените заданные по умолчанию параметры отчета и путь к каталогу, в котором будет сохранен отчет.
3. Нажмите **Выполнить скрипт** и выберите файл скрипта, который вам прислал оператор. Автоматически запустится выполнение утилиты с этим скриптом.

16. 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:

- ознакомьтесь с последними версиями описаний и руководств по адресу https://download.drweb.com/doc/;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу https://forum.drweb.com/index.php.

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

- заполните веб-форму в соответствующей секции раздела https://support.drweb.ru/fixit;
- 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/.

17. Приложение А. Пример использования

Здесь мы рассмотрим пример использования сервиса FixIt! для поиска и удаления троянской программы Trojan.AutoIt.289 на компьютере пользователя.

Описание проблемы

От пользователя поступила жалоба: по неизвестной причине не получалось открыть сайт антивируса и активировать демо-версию продукта.

Чтобы разобраться в проблеме, мы использовали сервис Dr.Web FixIt!.

Решение

Как всегда, мы начали с подготовки к работе с сервисом:

- завели задачу,
- создали анализирующую утилиту,
- отправили утилиту пользователю,
- получили аналитический отчет о состоянии компьютера.

Поскольку этот набор действий стандартен, мы не будем подробно описывать его в этом разделе. Информацию об этих этапах читайте в разделе Задача.

Работа с отчетом

Основная работа началась после получения отчета о состоянии компьютера.

Открыв отчет, мы перешли на вкладку **Поиск и анализ**, чтобы сразу отфильтровать вредоносные и подозрительные файлы.

Мы выбрали фильтры из раздела **General**:

- Downloaded files
- Scripting language interpreters
- New executables
- Rootkits
- Unsigned executables
- Files with unusual arkstatus
- Suspicious software
- Hacktools software
- Files with unusual certificates

фильтры из раздела **Detects**:

- Cloud URL detects
- Non-signature detects
- Signature detects
- Reputation-based detects

фильтр из раздела **Heuristics**:

- Unsigned untrusted executables

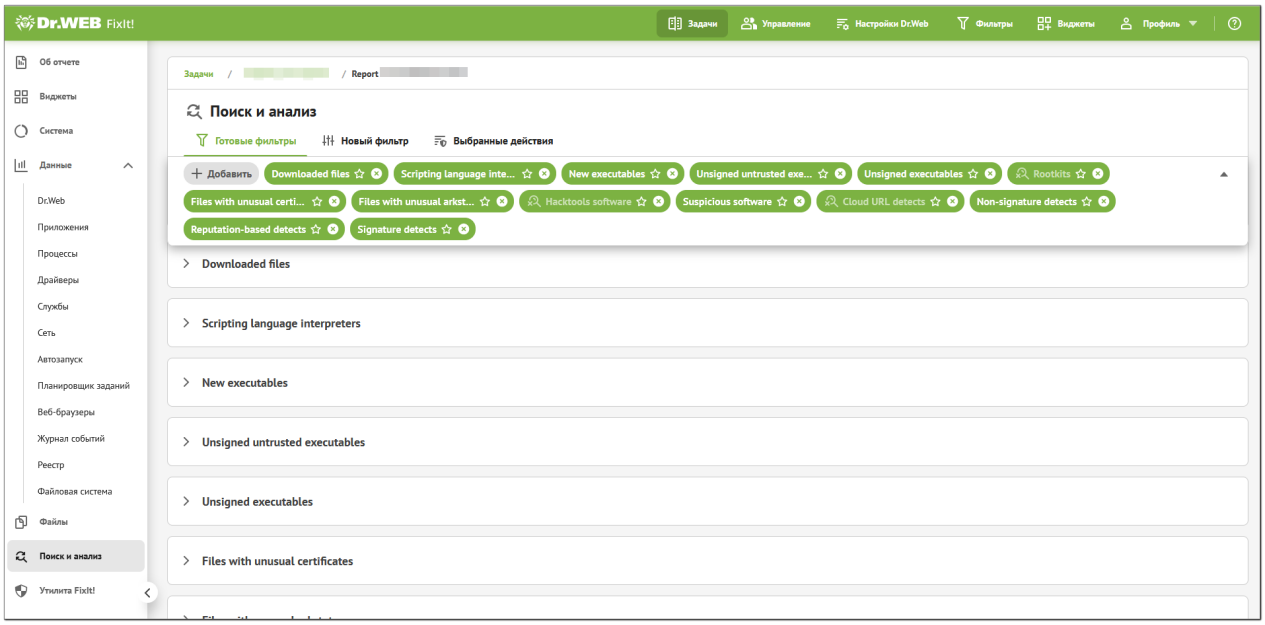

Рисунок 18. Выбранные фильтры

Это стандартный набор фильтров, который помогает выявить большинство угроз.

Фильтры из раздела **General** — эвристические; с их помощью мы ищем неподписанные, скрытые и просто подозрительные файлы. Наличие файла в таком фильтре само по себе не является гарантией того, что этот файл — вредоносный, но в сочетании с информацией из других фильтров уже можно делать выводы.

Фильтры из раздела **Detects** настроены таким образом, чтобы выявлять детектируемые вредоносные файлы. Поэтому мы начали поиск проблем именно с этих фильтров.

В нашем случае то, что нас интересует, обнаружилось в фильтре **Reputation-based detects**. В нем отображаются файлы, вошедшие в репутационную базу Metawave компании «Доктор Веб», — то есть те, что в какой-то момент были определены как зараженные, подозрительные, полученные от подозрительного поставщика или чистые.

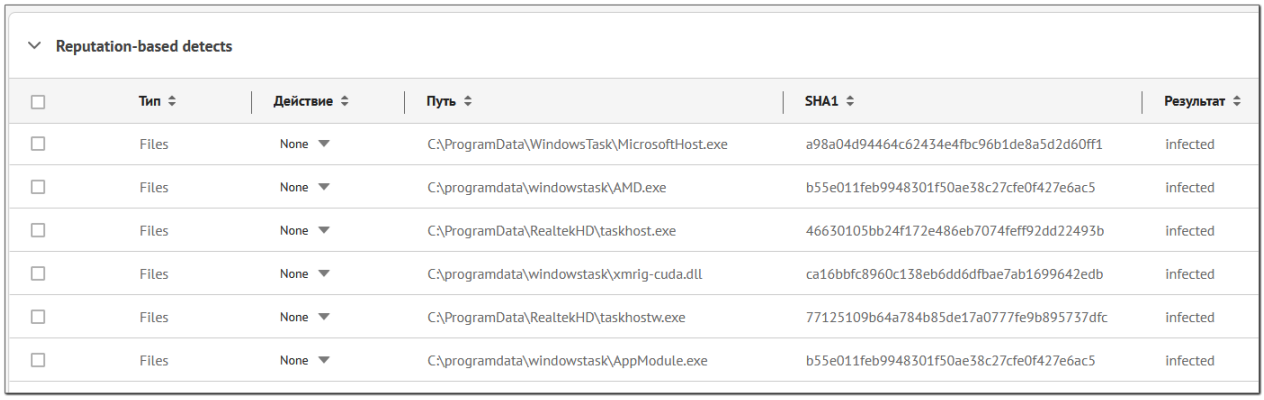

Рисунок 19. Фильтр Reputation-based detects

Здесь мы увидели несколько файлов с пометкой *infected*, включая известную вредоносную библиотеку `xmrig-cuda.dll`, но главная находка — это файл `C:\ProgramData\RealtekHD\taskhostw.exe`, визитная карточка трояна *Trojan.AutoIt.289*. Увидев этот файл, мы сделали вывод, что компьютер пользователя заражен именно этой вредоносной программой.

Для Trojan.AutoIt.289 в FixIt! создан специальный фильтр. Мы воспользовались им для поиска всех затронутых файлов и процессов.

Фильтр Trojan.AutoIt.289

Фильтр **Trojan.AutoIt.289** выводит все файлы, процессы и элементы автозагрузки, затронутые одноименным трояном.

Мы выбрали этот фильтр в списке на вкладке **Готовые фильтры** и раскрыли таблицу с результатами.

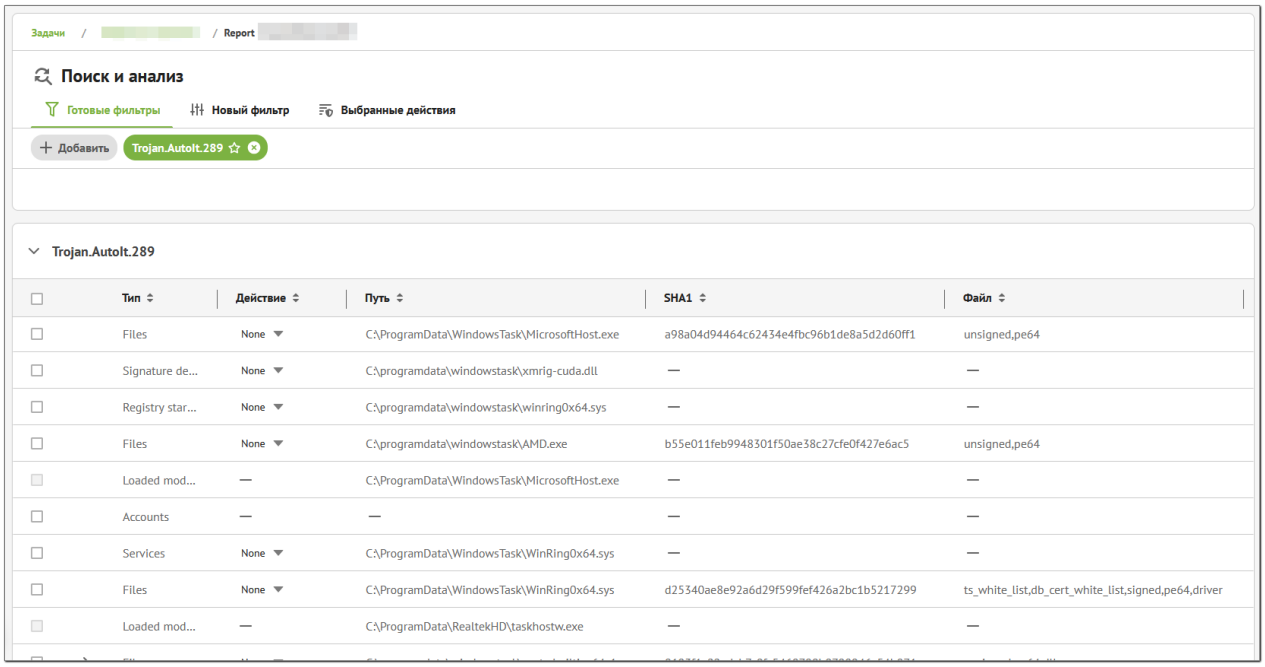

Рисунок 20. Фильтр Trojan.AutoIt.289

Все, что осталось сделать, — выбрать необходимое действие для найденных элементов.

Лечение

Действия для разных типов элементов различаются. Чтобы сгруппировать элементы, мы отметили флажком весь столбец. При этом отметились только те элементы, для которых доступно действие (например, для загруженных модулей действие не предусмотрено).

После этого в меню сверху мы поочередно выбрали тип элемента и действие для всех элементов этого типа.

Например, для типа **Processes** мы выбрали действие **Kill**.

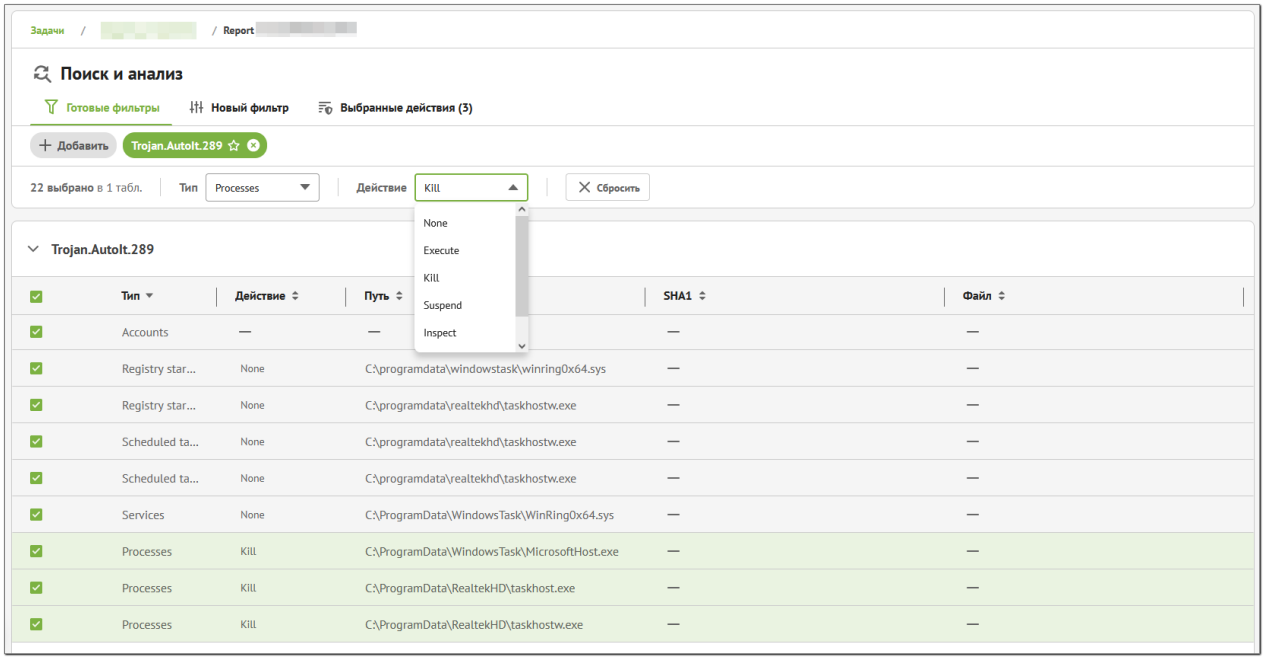

Рисунок 21. Выбор действий

Аналогичным образом мы поступили с элементами других типов, выбрав для них действия **Cure**, **Delete** и **Disinfect** соответственно.

Выбранные действия отобразились на одноименной вкладке, где их можно еще раз просмотреть и проверить.

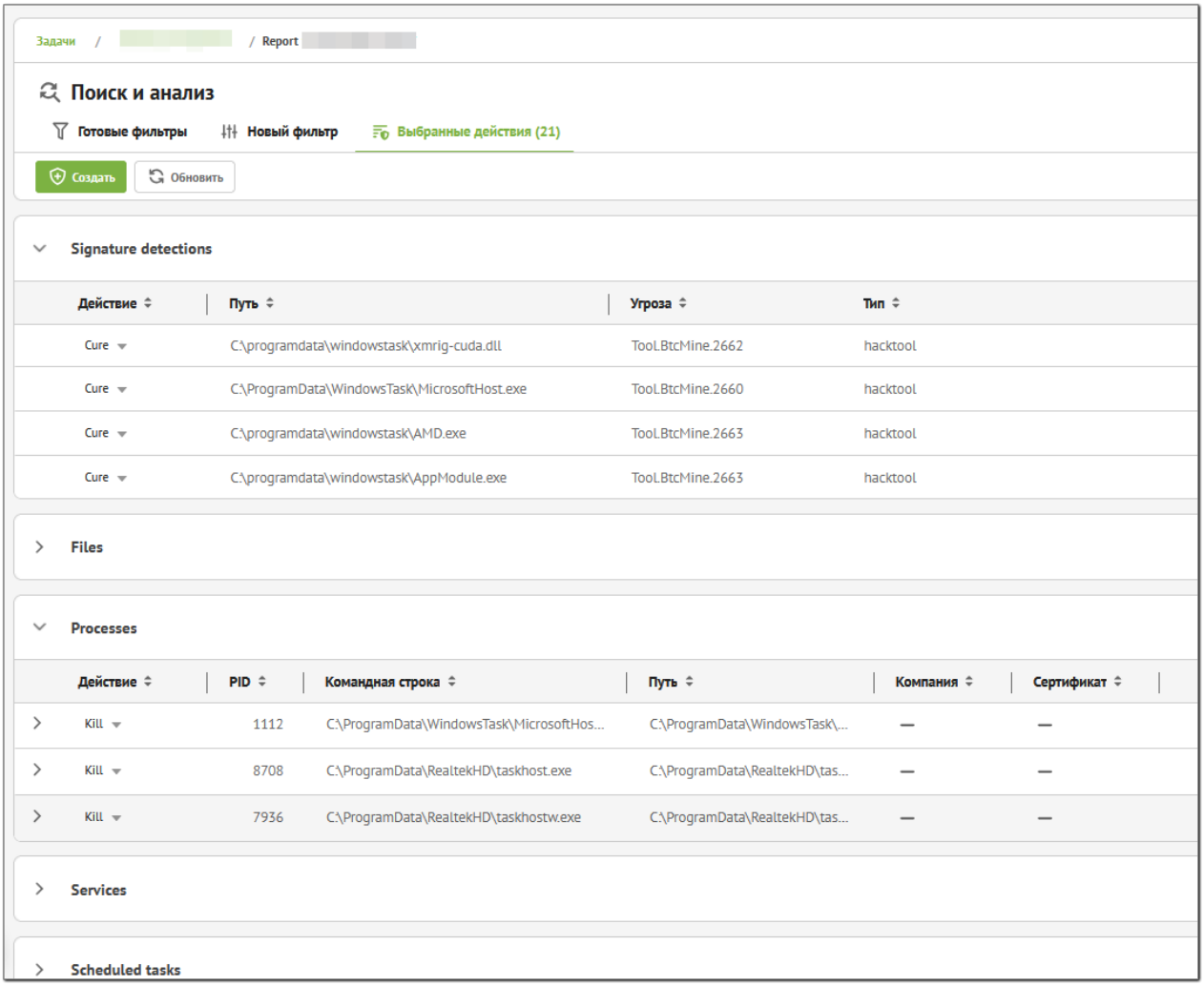

Рисунок 22. Выбранные действия

Убедившись, что все выбранные действия сохранились, мы нажали **Создать**, чтобы подготовить для пользователя лечащую утилиту.

Перед тем как создать утилиту, сервис FixIt! позволяет просмотреть полученный скрипт, в который можно также добавить команды вручную.

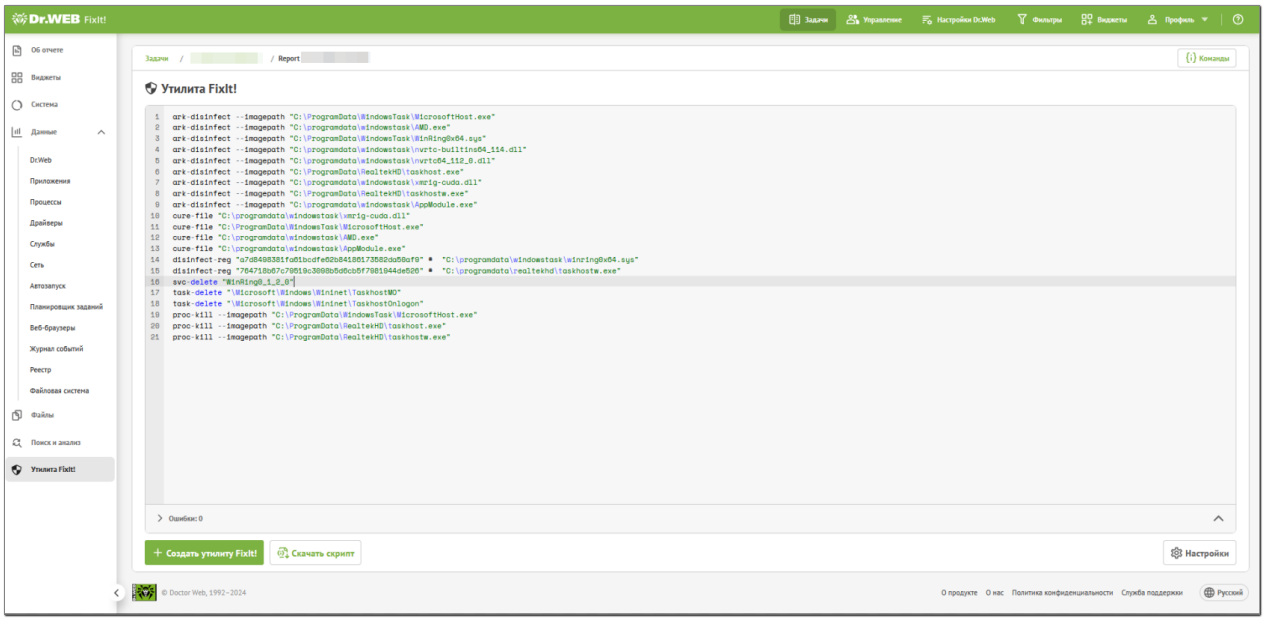

Рисунок 23. Готовый скрипт

Оптимизация

Несмотря на то, что скрипт выше полностью рабочий и способен решить найденные проблемы, более продвинутый пользователь FixIt! может его оптимизировать — либо на этапе выбора действий, либо на этапе проверки скрипта.

Что мы заметили:

- Логично поставить команды proc-kill в начало скрипта, поскольку все команды, за исключением -inspect, выполняются в том же порядке, в каком мы их расположили, и до лечения нам потребуется завершить процессы трояна.
- Команды cure-file и ark-disinfect в процессе выполнения завершают соответствующие вредоносным файлам процессы и удаляют элементы автозагрузки — то есть другие команды, которые отвечают за завершение процессов и удаление из автозагрузки, можно удалить из скрипта.
- Команды cure-file и ark-disinfect взаимозаменяемы, когда применяются к одному и тому же файлу, то есть могут дублировать друг друга. В нашем случае это произошло потому, что одни и те же объекты определились одновременно как **Signature detections** и как **Files**, то есть для них стали доступны разные варианты действий.

После удаления дублирующих друг друга команд скрипт стал выглядеть, как показано на следующем рисунке.

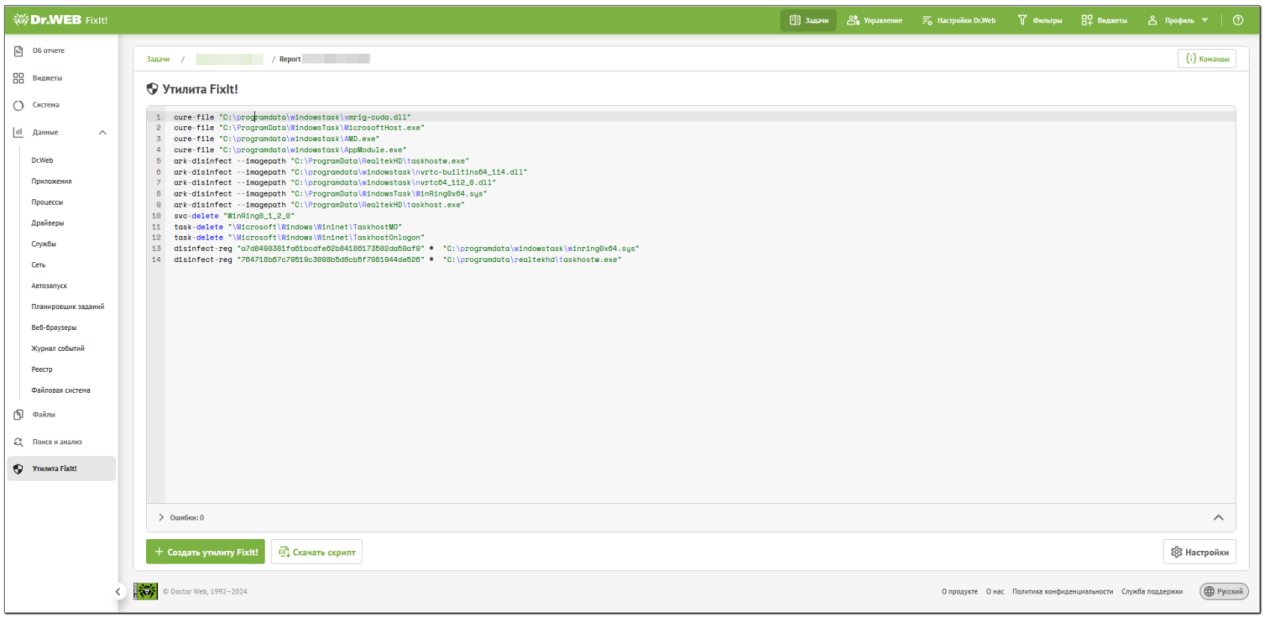

Рисунок 24. Скрипт после оптимизации

Еще раз нажав **Создать**, мы получили готовую лечащую утилиту и отправили ее пользователю.

Итог

Мы проанализировали отчет, сформированный после лечения, с помощью функции Сравнение отчетов и убедились, что угроза устранена.

18. Приложение Б. Список полей

- artefacts_fs
- defender:computer_status
- defender:preference
- defender:threat
- defender:threat_detection
- disk_bootsect
- drivers
- drweb:bases
- drweb:components
- drweb:info
- drweb:launched_modules
- drweb:licenses
- drweb:products
- events
- files
- fixes
- hosts
- installed_apps
- modules
- msi_apps
- net_connections
- net_providers:namespaces
- net_providers:protocols
- processes
- services
- startups:mstasks
- startups:registry
- startups:wmi
- sysobj:chromium_config
- sysobj:chromium_extensions
- sysobj:detects
- sysobj:firefox_addons
- sysobj:firefox_config

- sysobj:ie
- sysobj:mstasks
- sysobj:proxy
- sysobj:registry
- sysobj:shortcuts
- sysobj:wmi
- system:accounts
- system:antivirus
- system:bios
- system:cpu
- system:dep
- system:dirs
- system:dns
- system:firewall
- system:hdd
- system:kernel_va_shadowing
- system:locale
- system:machine_scores
- system:mapped_disks
- system:memory
- system:net_adapters
- system:os
- system:persisted_routes
- system:policies
- system:routes
- system:secure_boot
- system:security_providers
- system:sessions
- system:shares
- system:smart
- system:speculation_control
- system:user_privelegies
- system:users
- system_reg_export
- winstore_apps

artefacts_fs

Файловые артефакты

Поле	Тип данных
analysis_results.metawave.datetime	date
analysis_results.metawave.result	text
analysis_results.metawave.status	text
category_name	text
hash.sha1	text
modify_datetime	date
path	text
sha1	text
size	long

defender:computer_status

Состояние компьютера по данным Microsoft Defender

Поле	Тип данных
am_engine_version	keyword
am_product_version	keyword
am_service_enabled	boolean
am_service_version	keyword
antispyware_enabled	boolean
antispyware_signature_age	long

Поле	Тип данных
antispyware_signature_last_updated	date
antispyware_signature_version	keyword
antivirus_enabled	boolean
antivirus_signature_age	long
antivirus_signature_last_updated	date
antivirus_signature_version	keyword
behavior_monitor_enabled	boolean
category_name	text
computer_id	text
computer_state	long
full_scan_age	long
full_scan_end_time	text
full_scan_start_time	text
ioav_protection_enabled	boolean
last_full_scan_source	long
last_quick_scan_source	long
nis_enabled	boolean
nis_engine_version	keyword
nis_signature_age	long
nis_signature_last_updated	date

Поле	Тип данных
on_access_protection_enabled	boolean
quick_scan_age	long
quick_scan_end_time	date
quick_scan_start_time	date
real_time_protection_enabled	boolean
real_time_scan_direction	long

defender:preference

Настройки Microsoft Defender

Поле	Тип данных
category_name	text
check_for_signatures_before_running_scan	boolean
computer_id	text
disable_archive_scanning	boolean
disable_auto_exclusions	boolean
disable_behavior_monitoring	boolean
disable_catchup_full_scan	boolean
disable_catchup_quick_scan	boolean
disable_email_scanning	boolean
disable_intrusion_prevention_system	text
disable_ioav_protection	boolean

Поле	Тип данных
disable_privacy_mode	boolean
disable_realtime_monitoring	boolean
disable_removable_drive_scanning	boolean
disable_restore_point	boolean
disable_scanning_mapped_network_drives_for_full_scan	boolean
disable_scanning_network_files	boolean
disable_script_scanning	boolean
exclusion_path	text
high_threat_default_action	long
low_threat_default_action	long
maps_reporting	long
moderate_threat_default_action	long
quarantine_purge_items_after_delay	long
randomize_schedule_task_times	boolean
real_time_scan_direction	long
remediation_schedule_day	long
reporting_additional_action_time_out	long
reporting_critical_failure_time_out	long
reporting_non_critical_time_out	long
scan_only_if_idle_enabled	boolean

Поле	Тип данных
scan_parameters	long
scan_purge_items_after_delay	long
scan_schedule_day	long
scan_schedule_quick_scan_time	date
scan_schedule_time	date
severe_threat_default_action	long
signature_au_grace_period	long
signature_definition_update_file_shares_sources	text
signature_disable_update_on_startup_without_engine	boolean
signature_fallback_order	text
signature_first_au_grace_period	long
signature_schedule_day	long
signature_schedule_time	date
signature_update_catchup_interval	long
signature_update_interval	long
submit_samples_consent	long
ui_lockdown	boolean
unknown_threat_default_action	long

defender:threat

Угрозы, выявленные Microsoft Defender

Поле	Тип данных
category_id	long
category_name	text
did_threat_execute	boolean
is_active	boolean
resources	text
rollup_status	long
schema_version	keyword
severity_id	long
threat_id	long
threat_name	text
type_id	long

defender:threat_detection

Детектирование угрозы через Microsoft Defender

Поле	Тип данных
action_success	boolean
additional_actions_bit_mask	long
am_product_version	keyword
category_name	text

Поле	Тип данных
cleaning_action_id	long
current_threat_execution_status_id	long
detection_id	text
detection_source_type_id	long
domain_user	text
initial_detection_time	date
last_threat_status_change_time	date
process_name	text
remediation_time	text
resources	text
threat_id	long
threat_status_error_code	long
threat_status_id	long

disk_bootsect

Загрузочные сектора дисков

Поле	Тип данных
block.end_lba	text
block.start_lba	text
bytes_per_sector	integer
category_name	text

Поле	Тип данных
cylinders	integer
gpt.header.backup_lba	text
gpt.header.disk_guid	text
gpt.header.first_usable_lba	text
gpt.header.header_crc	text
gpt.header.header_size	text
gpt.header.last_usable_lba	text
gpt.header.num_parts	text
gpt.header.part_entries_crc	text
gpt.header.part_entry_lba	text
gpt.header.primary_lba	text
gpt.header.reserved	text
gpt.header.revision	text
gpt.header.signature	text
gpt.header.sizeof_part_entry	text
gpt.partition.arkstatus	text
gpt.partition.attrib	text
gpt.partition.end_lba	text
gpt.partition.guid	text
gpt.partition.index	text

Поле	Тип данных
gpt.partition.name	text
gpt.partition.start_lba	text
gpt.partition.type	text
id	integer
mbr.arkstatus	text
mbr.disk_signature	long
mbr.disk_signature	text
mbr.partition.arkstatus	text
mbr.partition.boot_id	integer
mbr.partition.boot_id	text
mbr.partition.index	integer
mbr.partition.index	text
mbr.partition.size_in_sectors	long
mbr.partition.size_in_sectors	text
mbr.partition.start_lba	long
mbr.partition.start_lba	text
mbr.partition.type	text
mbr.signature	integer
mbr.zero_padding	integer
media_type	integer

Поле	Тип данных
part_style	text
sectors_per_track	integer
size	long
tracks_per_cylinder	integer

drivers

Драйверы

Поле	Тип данных
base	text
category_name	text
path	text
size	long

drweb:bases

Антивирусные базы Dr.Web

Поле	Тип данных
category_name	text
name	text
path	text
records	long
timestamp	date

Поле	Тип данных
type	integer
version	text

drweb:components

Компоненты Dr.Web

Поле	Тип данных
category_name	text
installation_datetime	date
name	text

drweb:info

Информация о продукте Dr.Web

Поле	Тип данных
bases_path	text
category_name	text
hash	text
hash_sha1	text
install_path	text
product_mode	text
product_type	text
product_version	text

Поле	Тип данных
repo_path	text

drweb:launched_modules

Запущенные модули Dr.Web

Поле	Тип данных
launched	boolean

drweb:licenses

Лицензии Dr.Web

Поле	Тип данных
category_name	text
key.applications	text
key.created	date
key.expires	date
key.product_spec	text
key.product_type	text
key.products	text
key.subscription_expires	date
path	text
settings.app_control	text
settings.AppControl	text

Поле	Тип данных
settings.file_server	text
settings.FileServer	text
settings.inet_gateway	text
settings.InetGateway	text
settings.lotus_spam_filter	text
settings.LotusSpamFilter	text
settings.mail_server	text
settings.MailServer	text
settings.spam_filter	text
settings.SpamFilter	text
settings.Users	text
settings.users	text
user.computers	integer
user.name	text
user.number	text

drweb:products

Продукты Dr.Web

Поле	Тип данных
category_name	text
installation_datetime	date

Поле	Тип данных
name	text

engine_detects

Угрозы, выявленные по базе сигнатур

Поле	Тип данных
category_name	text
path	text
threat	text
type	text

events

События

Поле	Тип данных
category	text
category_name	text
code	text
computer	text
content	text
id	text
index	text
instance_id	text

Поле	Тип данных
keywords	text
logfile	text
msg	text
opcode	text
pid	text
source	text
task	text
tid	text
time	date
type	text
user	text

files

Файлы

Поле	Тип данных
analysis_results.metawave.datetime	date
analysis_results.metawave.result	text
analysis_results.metawave.status	text
arkstatus.cert	text
arkstatus.cloud	text
arkstatus.confidence	text

Поле	Тип данных
arkstatus.file	text
arkstatus.soft_type	text
arkstatus.soft_white	text
arkstatus.threat	text
arkstatus.type	text
atime	date
attrib.archive	boolean
attrib.compressed	text
attrib.dir	boolean
attrib.ea	text
attrib.hidden	boolean
attrib.invalid	boolean
attrib.normal	boolean
attrib.not_content_indexed	boolean
attrib.readonly	boolean
attrib.recall_on_open	text
attrib.reparse_point	text
attrib.security	text
attrib.sparse	text
attrib.system	boolean

Поле	Тип данных
attrib.temporary	boolean
attrib.value	text
buildtime	date
category_name	text
certinfo.catfile	text
certinfo.creator_name	text
certinfo.creator_url	text
certinfo.item.alg	text
certinfo.item.ca	text
certinfo.item.eku	text
certinfo.item.flags	text
certinfo.item.from	date
certinfo.item.hash_alg	text
certinfo.item.hash_alg_type	text
certinfo.item.issuer.C	text
certinfo.item.issuer.CN	text
certinfo.item.issuer.DC	text
certinfo.item.issuer.L	text
certinfo.item.issuer.O	text
certinfo.item.issuer.OU	text

Поле	Тип данных
certinfo.item.issuer.ST	text
certinfo.item.sn	text
certinfo.item.subject.C	text
certinfo.item.subject.CN	text
certinfo.item.subject.DC	text
certinfo.item.subject.L	text
certinfo.item.subject.O	text
certinfo.item.subject.OU	text
certinfo.item.subject.SERIALNUMBER	text
certinfo.item.subject.ST	text
certinfo.item.thumbprint	text
certinfo.item.thumbprint_sha256	text
certinfo.item.to	date
certinfo.timestamp	date
certinfo.type	text
ctime	date
device_characteristics	text
device_type	text
eainfo.item.data	text
eainfo.item.name	text

Поле	Тип данных
eainfo.item.size	text
easize	integer
hash.pemd5	text
hash.pesha1	text
hash.pesha256	text
hash.pesha512	text
hash.sha1	text
hash.sha256	text
links	integer
path	text
signed	boolean
size	long
verinfo.company	text
verinfo.descr	text
verinfo.file_version_num	text
verinfo.origname	text
verinfo.product_name	text
verinfo.product_version	text
verinfo.product_version_num	text
verinfo.version	text

Поле	Тип данных
wtime	date
zone_transfer.host_url	text
zone_transfer.id	text
zone_transfer.referrer_url	text
zone_transfer.package_name	text

fixes

Исправления

Поле	Тип данных
__type__	text
caption	text
category.id	text
category.name	text
category_name	text
comment	text
csname	text
descr	text
hidden	text
id	text
installed_by	text
installed_on	date

Поле	Тип данных
need_reboot	text

hosts

Хосты

Поле	Тип данных
category_name	text
ip.address	ip
ip.category	text
ip.domain.address	text
ip.domain.category	text
line	integer
path	text
text	text

installed_apps

Установленные приложения

Поле	Тип данных
category_name	text
hidden	text
id	text
location	text

Поле	Тип данных
name	text
uninstall	text

modules

Модули

Поле	Тип данных
category_name	text
path	text

msi_apps

Приложения MSI

Поле	Тип данных
category_name	text
id	text
language	integer
msi_package_code	text
msi_product_code	text
name	text
vendor	text
version	text

net_connections

Сетевые подключения

Поле	Тип данных
__type__	text
category_name	text
local_addr	ip
local_port	integer
local_scopeid	text
path	text
pid	integer
remote_addr	ip
remote_port	integer
remote_scopeid	text
state	text

net_providers:namespaces

Провайдеры сети (пространства имен)

Поле	Тип данных
active	boolean
broken	boolean
category_name	text
guid	text

Поле	Тип данных
name	text
namespace	text
path	text
version	text
wow64	boolean

net_providers:protocols

Провайдеры сети (протоколы)

Поле	Тип данных
broken	boolean
category_name	text
entryid	text
flags	text
guid	text
name	text
path	text
protocol	text
scheme	text
version	text
wow64	boolean

processes

Процессы

Поле	Тип данных
appid	text
base	text
bit	integer
category_name	text
cmdline	text
create_time	date
curdir	text
handles	integer
ilevel	text
isdebugged	boolean
kernel_time	text
memory_usage.other_op	long
memory_usage.pagefaults	long
memory_usage.pagefile_usage	long
memory_usage.peak_pagefile_usage	long
memory_usage.peak_virtual_size	long
memory_usage.peak_workingset	long
memory_usage.quota_non_pagedpool	long

Поле	Тип данных
memory_usage.quota_pagedpool	long
memory_usage.quota_peak_non_pagedpool	long
memory_usage.quota_peak_pagedpool	long
memory_usage.read_op	long
memory_usage.virtual_size	long
memory_usage.workingset	long
memory_usage.write_op	long
mitigations.aslr_policy.disallow_stripped_images	text
mitigations.aslr_policy.enable_bottom_up_randomization	text
mitigations.aslr_policy.enable_force_relocate_images	text
mitigations.aslr_policy.enable_high_entropy	text
mitigations.cfg_policy.enable_cfg	text
mitigations.cfg_policy.enable_export_suppression	text
mitigations.cfg_policy.strict_mode	text
mitigations.child_process_policy.allow_secure_process_creation	text
mitigations.child_process_policy.audit_no_child_process_creation	text
mitigations.child_process_policy.no_child_process_creation	text
mitigations.dynamic_code_policy.allow_remote_downgrade	text
mitigations.dynamic_code_policy.allow_thread_opt_out	text

Поле	Тип данных
mitigations.dynamic_code_policy.audit_prohibit_dynamic_code	text
mitigations.dynamic_code_policy.prohibit_dynamic_code	text
mitigations.extension_point_disable_policy.disable_extension_points	text
mitigations.font_disable_policy.audit_non_system_font_loading	text
mitigations.font_disable_policy.disable_non_system_fonts	text
mitigations.image_load_policy.audit_no_low_mandatory_label_images	text
mitigations.image_load_policy.audit_no_remote_images	text
mitigations.image_load_policy.no_low_mandatory_label_images	text
mitigations.image_load_policy.no_remote_images	text
mitigations.image_load_policy.prefer_system32_images	text
mitigations.payload_restriction_policy.audit_export_address_filter	text
mitigations.payload_restriction_policy.audit_export_address_filter_plus	text
mitigations.payload_restriction_policy.audit_import_address_filter	text
mitigations.payload_restriction_policy.audit_rop_caller_check	text
mitigations.payload_restriction_policy.audit_rop_sim_exec	text
mitigations.payload_restriction_policy.audit_rop_stack_pivot	text

Поле	Тип данных
mitigations.payload_restriction_policy.enable_export_address_filter	text
mitigations.payload_restriction_policy.enable_export_address_filter_plus	text
mitigations.payload_restriction_policy.enable_import_address_filter	text
mitigations.payload_restriction_policy.enable_rop_caller_check	text
mitigations.payload_restriction_policy.enable_rop_sim_exec	text
mitigations.payload_restriction_policy.enable_rop_stack_pivot	text
mitigations.redirection_trust_policy.audit_redirectiont_rust	text
mitigations.redirection_trust_policy.enforce_redirection_trust	text
mitigations.side_channel_isolation_policy.disable_page_combine	text
mitigations.side_channel_isolation_policy.isolate_security_domain	text
mitigations.side_channel_isolation_policy.smt_branch_target_isolation	text
mitigations.side_channel_isolation_policy.speculative_store_bypass_disable	text
mitigations.signature_policy.audit_microsoft_signed_only	text
mitigations.signature_policy.audit_store_signed_only	text
mitigations.signature_policy.microsoft_signed_only	text
mitigations.signature_policy.mitigation_opt_in	text

Поле	Тип данных
mitigations.signature_policy.store_signed_only	text
mitigations.strict_handle_check_policy.handle_exceptions_permanently_enabled	text
mitigations.strict_handle_check_policy.raise_exception_on_invalid_handle_reference	text
mitigations.syscall_disable_policy.audit_disallow_win32k_syscalls	text
mitigations.syscall_disable_policy.disallow_win32k_syscalls	text
mitigations.systemcall_filter_policy.filter_id	text
mitigations.user_shadow_stack_policy.audit	text
mitigations.user_shadow_stack_policy.audit_block_non_cet_binaries	text
mitigations.user_shadow_stack_policy.audit_set_context_ip_validation	text
mitigations.user_shadow_stack_policy.block_non_cet_binaries	text
mitigations.user_shadow_stack_policy.block_non_cet_binaries_non_ehcont	text
mitigations.user_shadow_stack_policy.cet_dynamic_apis_out_of_proc_only	text
mitigations.user_shadow_stack_policy.enable	text
mitigations.user_shadow_stack_policy.enable_strict_mode	text
mitigations.user_shadow_stack_policy.set_context_ip_validation	text
mitigations.user_shadow_stack_policy.set_context_ip_validation_relaxed_mode	text

Поле	Тип данных
module.arkstatus	text
module.base	text
module.buildtime	date
module.path	text
module.size	long
path	text
peb	text
pid	integer
ppid	integer
priority	integer
protection_level	text
section_info.checksum	text
section_info.committed_stack_size	long
section_info.dll_characteristics	text
section_info.image_characteristics	text
section_info.image_contains_code	boolean
section_info.image_file_size	long
section_info.image_flags	text
section_info.loader_flags	text
section_info.machine	text

Поле	Тип данных
section_info.max_stack_size	long
section_info.os_major_ver	text
section_info.os_minor_ver	text
section_info.subsystem	text
section_info.subsystem_major_ver	text
section_info.subsystem_minor_ver	text
section_info.transfer_address	text
section_info.zero_bits	text
session_id	text
shell_info	text
shortcut	text
size	long
threads.count	text
threads.thread.base_priority	text
threads.thread.create_time	text
threads.thread.kernel_time	text
threads.thread.path	text
threads.thread.priority	text
threads.thread.start_address	text
threads.thread.state	text

Поле	Тип данных
threads.thread.tid	text
threads.thread.user_time	text
threads.thread.win32_start_address	text
title	text
type	text
unique_id	text
user_time	text
window_flags	text

services

Службы

Поле	Тип данных
category_name	text
checkpoint	text
cmdline	text
controls_accepted	text
depends	text
display_name	text
error_control	text
flags	text
group	text

Поле	Тип данных
name	text
path	text
pid	integer
start_name	text
startmode	text
state	text
svc_exitcode	text
tagid	text
type	text
waithint	text
win32_exitcode	text

startups:mstasks

Элементы автозагрузки (задачи планировщика заданий)

Поле	Тип данных
args	text
category_name	text
clsid	text
command	text
enabled	text
is_job	text

Поле	Тип данных
name	text
path	text
state	text
type	text
workdir	text

startups:registry

Элементы автозагрузки (реестр)

Поле	Тип данных
arkstatus	text
category_name	text
clsid	text
data	text
id	text
full_key	text
key	text
path	text
sid	text
value	text

startups:wmi

Элементы автозагрузки (WMI)

Поле	Тип данных
arkstatus	text
category_name	text
class	text
clsid	text
instance	text
name	text
namespace	text
path	text
value	text
workdir	text

sysobj:chromium_config

Системные объекты (настройки Chromium)

Поле	Тип данных
browser	text
category_name	text
profile	text
sid	text
url	text

sysobj:chromium_extensions

Системные объекты (расширения Chromium)

Поле	Тип данных
browser	text
category_name	text
id	text
name	text
path	text
profile	text
sid	text
url	text
version	text

sysobj:detects

Системные объекты (выявленные угрозы)

Поле	Тип данных
category_name	text
data	text
id	text
object	text
path	text
threat	text

Поле	Тип данных
type	text

sysobj:firefox_addons

Системные объекты (дополнения Firefox)

Поле	Тип данных
browser	text
category_name	text
id	text
name	text
path	text
profile	text
sid	text
type	text
url	text
version	text

sysobj:firefox_config

Системные объекты (настройки Firefox)

Поле	Тип данных
browser	text
category_name	text

Поле	Тип данных
profile	text
sid	text
url	text

sysobj:ie

Системные объекты

Поле	Тип данных
category_name	text
data	text
id	text
key	text
sid	text
value	text

sysobj:mstasks

Системные объекты (задачи планировщика заданий)

Поле	Тип данных
category_name	text
clsid	text
command	text
enabled	text

Поле	Тип данных
is_job	text
name	text
path	text
state	text
type	text
workdir	text

sysobj:proxy

Системные объекты (прокси)

Поле	Тип данных
category_name	text
data	text
id	text
key	text
sid	text
value	text

sysobj:registry

Системные объекты (реестр)

Поле	Тип данных
arkstatus	text

Поле	Тип данных
category_name	text
clsid	text
data	text
full_key	text
id	text
key	text
path	text
sid	text
threat	text
value	text

sysobj:shortcuts

Системные объекты (ярлыки)

Поле	Тип данных
arg	text
arkstatus	text
category_name	text
data	text
mac	text
machine_id	text
name	text

Поле	Тип данных
path	text
relative	text
target	text
threat	text
workdir	text

sysobj:wmi

Системные объекты (WMI)

Поле	Тип данных
arkstatus	text
category_name	text
class	text
clsid	text
data	text
instance	text
name	text
namespace	text
path	text
threat	text
value	text
workdir	text

system_reg_export

Реестр

Поле	Тип данных
arkstatus	text
category_name	text
hive	text
lastwrite	date
name	text
security	text
subkeys	integer
value.arkstatus	text
value.name	text
value.size	integer
value.type	text
value.value	text
values	integer

system:accounts

Данные о системе (учетные записи)

Поле	Тип данных
bad_passwd_count	integer
category_name	text

Поле	Тип данных
codepage	text
country	text
descr	text
expires	date
flags	text
fullname	text
group.name	text
home	text
home_drive	text
last_logoff	text
last_logon	date
logons_count	integer
logons_server	text
name	text
password_age	text
profile	text
script	text
type	text
workstation	text

system:antivirus

Данные о системе (антивирус)

Поле	Тип данных
category_name	text
company	text
enabled	boolean
guid	text
name	text
product_exe	text
product_exe_company	text
product_exe_version	text
reporting_exe	text
reporting_exe_company	text
reporting_exe_version	text
timestamp	text
uptodate	boolean
version	text

system:bios

Данные о системе (BIOS)

Поле	Тип данных
category_name	text

Поле	Тип данных
manufacturer	text
primary	text
release_date	date
system_bios_major	integer
system_bios_minor	integer
version	text

system:cpu

Данные о системе (ЦП)

Поле	Тип данных
category_name	text
cores	integer
cpuid	text
descr	text
enabled_cores	text
id	text
load	text
logical_cpus	long
manufacturer	text
max_speed	integer
name	text

Поле	Тип данных
socket	text
speed	integer
threads	integer
vmmonitor_support	boolean
vt_support	boolean

system:dep

Поле	Тип данных
available	boolean
category_name	text
for_32bit	boolean
for_drivers	boolean
policy	integer

system:dirs

Данные о системе (каталоги)

Поле	Тип данных
category_name	text
name	text
path	text

system:dns

DNS системы

Поле	Тип данных
category_name	text
name	text
server	text

system:firewall

Данные о системе (брандмауэр)

Поле	Тип данных
category_name	text
company	text
enabled	boolean
guid	text
name	text
product_exe	text
product_exe_company	text
product_exe_version	text
reporting_exe	text
reporting_exe_company	text
reporting_exe_version	text
timestamp	text

Поле	Тип данных
version	text

system:hdd

Данные о системе (жесткий диск)

Поле	Тип данных
category_name	text
deviceid	text
firmware	text
model	text
name	text
partition.block_size	long
partition.bootable	boolean
partition.bootpart	boolean
partition.id	text
partition.index	text
partition.primary	boolean
partition.size	long
partition.start_offset	long
partition.type	text
partition.volume.compressed	boolean
partition.volume.descr	text

Поле	Тип данных
partition.volume.dirty	boolean
partition.volume.drive	text
partition.volume.drive_type	text
partition.volume.free	long
partition.volume.fs_type	text
partition.volume.media_type	text
partition.volume.name	text
partition.volume.serial	text
partition.volume.size	long
partitions	integer
serial	text
size	long
type	text

system:kernel_va_shadowing

Поле	Тип данных
category_name	text
enabled	boolean
flags	integer
invalid_pte_bit	text
invpcid	text

Поле	Тип данных
invpcid_flushing_optimization	boolean
l1_data_cache_flush_supported	text
l1_terminal_fault_mitigation_present	text
pcid	text
pcid_flushing_optimization	boolean
required	text
required_available	text
status	text
user_global	text
user_pages_marked_global	boolean

system:locale

Данные о системе (локаль)

Поле	Тип данных
category_name	text
code	text
codeset	text
country	text
descr	text
name	text
oslang	text

system:machine_scores

Данные о системе (индекс производительности)

Поле	Тип данных
category_name	text
cpu	float
direct3d	float
disk	float
graphics	float
memory	float
timetaken	text
winsat_state	text
winsprlevel	float

system:mapped_disks

Данные о системе (сопоставленные диски)

Поле	Тип данных
category_name	text
drive	text
free	text
fs_type	text
item.drive	text
item.free	text

Поле	Тип данных
item.fs_type	text
item.path	text
item.session_id	text
item.size	text
item.volume_name	text
path	text
session_id	text
size	text
volume_name	text

system:memory

Данные о системе (оперативная память)

Поле	Тип данных
category_name	text
free	long
free_virtual	long
total	long
total_virtual	long

system:net_adapters

Сеть (интерфейсы)

Поле	Тип данных
category_name	text
default_ip_gateway	ip
dhcp_enabled	boolean
dhcp_server	ip
dns	text
dns_server_search_order	ip
id	text
index	text
ip_enabled	boolean
mac	text
name	text
subnet	ip

system:os

Данные о системе (ОС)

Поле	Тип данных
bit	integer
boot_device	text
boot_mode	text

Поле	Тип данных
build	text
category_name	text
code_integrity	text
debug	boolean
install_date	date
last_bootup_time	date
local_time	date
name	text
pae	text
sp	text
suite	text
type	text
version	text

system:persisted_routes

Поле	Тип данных
caption	text
category_name	text
descr	text
destination	text
item.caption	text

Поле	Тип данных
item.descr	text
item.destination	text
item.mask	text
item.metric1	text
item.name	text
item.next_hop	text
mask	text
metric1	text
name	text
next_hop	text

system:policies

Политики системы

Поле	Тип данных
__type__	text
category_name	text
full_key	text
key.item.name	text
key.item.size	integer
key.item.value	text
key.name	text

Поле	Тип данных
name	text
sid	text
value.name	text
value.size	text
value.value	text

system:recovery

Поле	Тип данных
auto_reboot	boolean
category_name	text
dump_path	text
dump_type	integer
kernel_dump_only	boolean
mini_dump_dir	text
overwrite_existing_dump	boolean
send_admin_alert	boolean
write_debug_info	boolean
write_to_eventlog	boolean

system:routes

Данные о сети (статические маршруты)

Поле	Тип данных
age	text
caption	ip
category_name	text
descr	text
destination	ip
information	text
interface_index	text
mask	ip
metric1	text
metric2	text
metric3	text
metric4	text
metric5	text
name	ip
next_hop	ip
protocol	text
type	text

system:secure_boot

Поле	Тип данных
capable	boolean
category_name	text
enabled	boolean

system:security_providers

Поле	Тип данных
category_name	text
health	text
name	text

system:sessions

Данные о системе (сеансы)

Поле	Тип данных
category_name	text
client_device_id	text
client_dir	text
client_ip	text
client_name	text
connect_time	date
disconnect_time	date

Поле	Тип данных
domain	text
envid	text
id	text
is_rdp	text
last_input_time	date
logon_time	date
name	text
remote_ip	text
state	text
station_name	text
user	text

system:shares

Данные о системе (общие каталоги)

Поле	Тип данных
caption	text
category_name	text
descr	text
name	text
path	text
type	integer

system:smart

Атрибуты S.M.A.R.T.

Поле	Тип данных
attribute.index	integer
attribute.name	text
attribute.raw	integer
attribute.threshold	integer
attribute.value	integer
attribute.worst	integer
category_name	text
firmware	text
id	text
model	text
serial_number	text

system:speculation_control

Поле	Тип данных
bpb_disabled_kernel_to_user	text
bpb_disabled_no_hardware_support	text
bpb_disabled_system_policy	text
bpb_enabled	text

Поле	Тип данных
branch_prediction_mitigation.disabled_by_system_policy	boolean
branch_prediction_mitigation.disabled_no_microcode_update	boolean
branch_prediction_mitigation.enabled	boolean
category_name	text
cpu_microcode_support_pred_cmd.enabled	boolean
cpu_microcode_support_pred_cmd.window_use_ibpb	boolean
cpu_microcode_support_spec_ctrl.enabled	boolean
cpu_microcode_support_spec_ctrl.windows_use_ibrs	boolean
cpu_microcode_support_spec_ctrl.windows_use_stipb	boolean
enhanced_ibrs	text
enhanced_ibrs_reported	text
flags	long
hv_l1tf_migitation_enabled	text
hv_l1tf_migitation_not_enabled_hardware	text
hv_l1tf_migitation_not_enabled_load_option	text
hv_l1tf_processor_not_affected	text
hv_l1tf_status_available	text
hvl_1tf_migitation_not_enabled_core_scheduler	text
ibrs_present	text
mb_clear_enabled	text

Поле	Тип данных
mb_clear_reported	text
mds_hardware_protected	text
smep_present	text
spec_cmd_enumerated	text
spec_ctrl_enumerated	text
spec_ctrl_import_optimization_enabled	text
spec_ctrl_retpoline_enabled	text
speculative_store_bypas_sdisable_supported	text
speculative_store_bypass_disable_available	text
speculative_store_bypass_disable_required	text
speculative_store_bypass_disable_supported	text
speculative_store_bypass_disabled_kernel	text
speculative_store_bypass_disabled_system_wide	text
status	text
stibp_present	text

system:user_privelegies

Права пользователя в системе

Поле	Тип данных
category_name	text
enabled	boolean

Поле	Тип данных
name	text

system:users

Данные о системе (пользователи)

Поле	Тип данных
category_name	text
folder.name	text
folder.path	text
home	text
name	text
network_drive.connect_flags	text
network_drive.connection_type	text
network_drive.defer_flags	text
network_drive.letter	text
network_drive.provider_name	text
network_drive.provider_type	text
network_drive.remote_path	text
network_drive.username	text
sid	text
type	integer

winstore_apps

Приложения из магазина Microsoft Store

Поле	Тип данных
arch	text
category_name	text
id	text
name	text
vendor.C	text
vendor.CN	text
vendor.L	text
vendor.O	text
vendor.OID.1.3.6.1.4.1.311.60.2.1.2	text
vendor.OID.1.3.6.1.4.1.311.60.2.1.3	text
vendor.OID.2.5.4.15	text
vendor.OU	text
vendor.S	text
vendor.SERIALNUMBER	text
version	text