Dr.WEB

FixIt!

Руководство пользователя

Dr.Web FixIt!
Версия 2.3
Руководство пользователя
05.04.2024

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

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! — веб-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 веб-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. В веб-сервисе вы создаете задачу и отправляете анализирующую утилиту FixIt! владельцу проверяемого компьютера.
2. Владелец проверяемого компьютера запускает утилиту FixIt!. Утилита проверяет компьютер и формирует отчет.
3. В веб-сервисе вы анализируете отчет, 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, объединенных принадлежностью к какой-либо категории (организации, отделу и т.п.). Пользователи

могут создавать свои задачи и просматривать другие задачи внутри своего пространства.

3. Системные требования

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

Параметр	Требование
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	Требование
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,

	• Windows 8, • Windows 8.1, • Windows 10, • Windows 11
Место на жестком диске	Не менее 1 ГБ
Свободная оперативная память	256 МБ и больше

4. Начало работы

Для начала работы с Dr.Web FixIt! необходимо приобрести лицензию и авторизоваться в веб-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 кнопку **Войти**.

Если пользователь не совершает никаких действий в сервисе в течение 1 часа и флажок **Запомнить меня** не установлен, сеанс автоматически завершается с переходом на главную страницу. При этом внизу страницы отображается 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

- В выпадающем списке **Язык интерфейса** выберите предпочитаемый язык. Язык интерфейса изменится автоматически.

Чтобы изменить пароль

1. Нажмите **Редактировать**.

2. Введите текущий пароль, а затем новый. Повторите новый пароль, чтобы избежать ошибок.
3. 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.

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 активировать пространства,
  - устанавливать лимит на создание задач в пространстве;
  - задавать время жизни задач для пространства;
  - добавлять связанные пространства, с которыми можно делиться задачами;
  - просматривать списки пространств, связанных с другими пространствами.
- управлять учетными записями:
  - создавать новых администраторов,
  - создавать новых 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 новых 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,
    - вносить изменения в фильтры,
    - добавлять фильтры в группы.

5.3. Пользователь

Пользователь имеет доступ ко всем задачам пространства, к которому он принадлежит. Он может:

- вносить изменения в свой список задач:
    - открывать новые 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,
  - вносить изменения в фильтры,
  - добавлять фильтры в группы.

6. Управление

Раздел **Управление** позволяет управлять пространствами и учетными записями администраторов. Раздел доступен только администраторам. Менеджерам и пользователям вместо раздела **Управление** доступен раздел Пространство.

Раздел **Управление** содержит две вкладки — **Пространства** и **Администраторы**.

На вкладке **Пространства** администратору доступен полный список пространств сервиса. Администратор может создавать пространства, просматривать информацию о них, добавлять связанные пространства, редактировать и блокировать пространства.

На вкладке **Администраторы** можно создать новую учетную запись администратора, а также отредактировать или удалить уже имеющуюся.

6.1. Пространства

Вкладка **Пространства** содержит сводную таблицу всех пространств сервиса. Для каждого пространства в таблице доступна следующая информация:

- **Пространство**: имя пространства.
- **Статус**: Активно или Заблокировано.
- **Использовано задач**: количество задач, использованных в данном пространстве. Если лимит для пространства не задан, столбец содержит значение Безлимитно.
- **Участники**: суммарное количество менеджеров и пользователей пространства.
- **Последнее изменение**: дата и время последнего изменения, внесенного в пространство.

Нажмите на имя пространства в столбце **Пространство**, чтобы перейти на страницу с подробной информацией о пространстве.

Фильтрация и поиск

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

Таблицу можно фильтровать по следующим параметрам пространства:

- имя,
- статус,
- последнее изменение.

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

Чтобы задать фильтр для таблицы пространств

1. Нажмите на значок **Фильтр** над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Имя** или **Статус**:
   - Установите флажки напротив интересующих вас значений.

   Если вы выбрали параметр **Последнее изменение**:
   - Нажмите на интересующие вас даты. Чтобы задать период времени, нажмите на дату начала периода и потяните курсор до даты окончания периода (см. Рисунок 1).
4. Нажмите кнопку **Применить**.

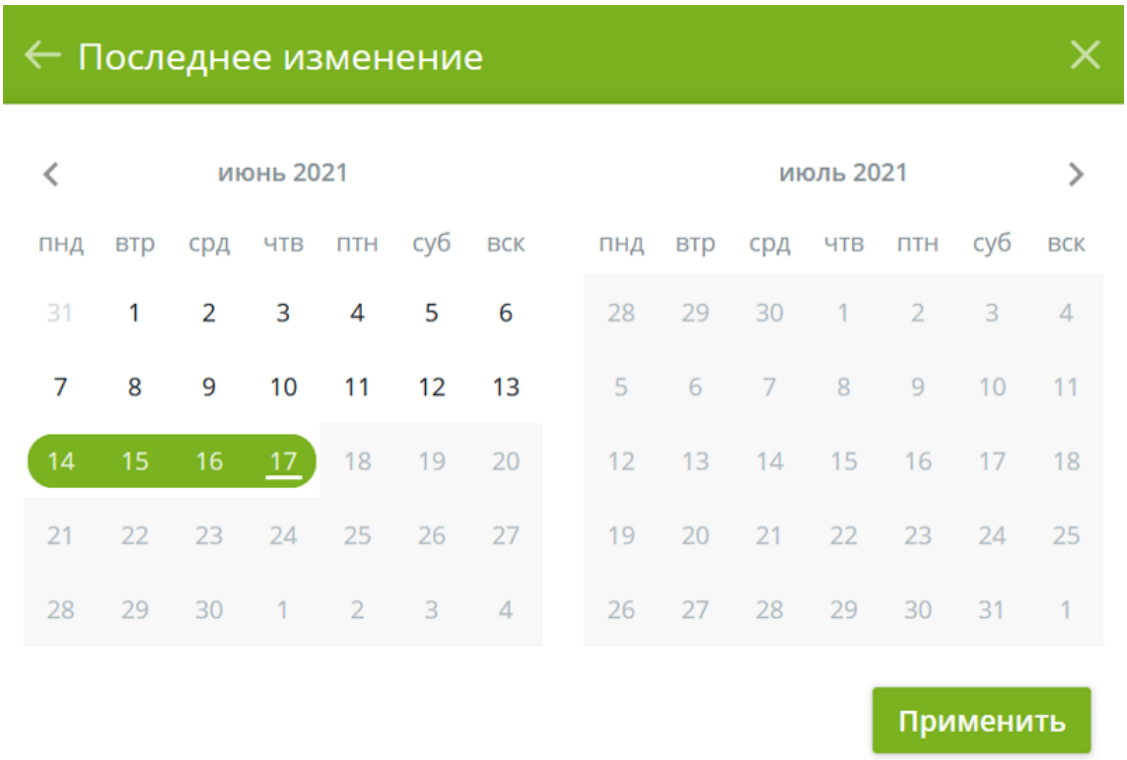

Рисунок 1. Фильтрация по периоду

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

Чтобы выполнить поиск по таблице пространств

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 пространствами

На вкладке **Пространства** администратор также может управлять пространствами сервиса: создать новое пространство, редактировать, заблокировать или разблокировать существующее.

Чтобы создать пространство

1. Нажмите кнопку  над таблицей.
2. Во всплывающем окне **Новое пространство** в поле **Имя** укажите имя нового пространства.
3. При необходимости вы можете установить лимит на количество задач в пространстве. Для этого установите флажок **Установить лимит задач** и укажите необходимое количество в поле **Лимит**.
4. Нажмите кнопку **Сохранить**.

Чтобы редактировать пространство

1. Наведите курсор на строку с нужным пространством и нажмите  в правой части строки (см. Рисунок 2).
2. Во всплывающем окне **Редактировать пространство** внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

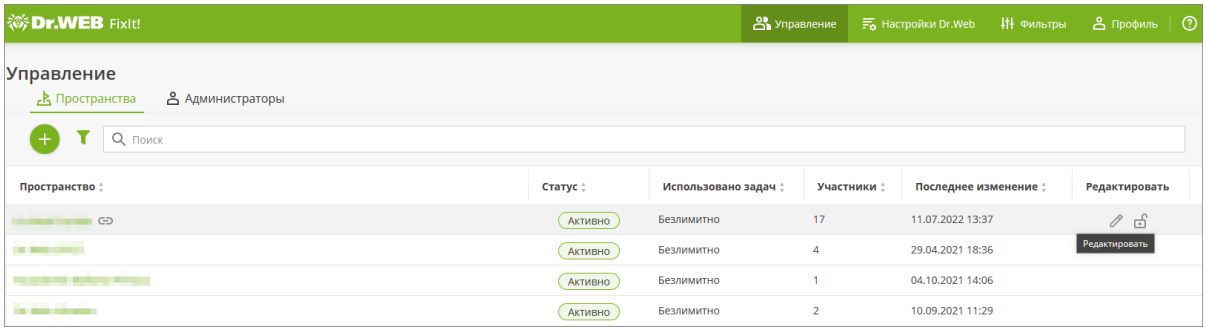

Рисунок 2. Редактирование пространства

Пространство можно заблокировать, если сотрудничество с его участниками по той или иной причине завершено. В случае блокировки пространства продолжить работу над его задачами будет невозможно.

Чтобы заблокировать пространство

1. Наведите курсор на строку с нужным пространством и нажмите в правой части строки.
2. Во всплывающем окне **Заблокировать пространство** подтвердите блокировку.

> Менеджеры и пользователи не смогут работать в пространстве после его блокировки.

Чтобы разблокировать пространство

- Наведите курсор на строку с нужным пространством и нажмите в правой части строки.

> Разблокировать пространство могут только администраторы.

6.2. Администраторы

Вкладка **Администраторы** содержит сводную таблицу всех администраторов сервиса. Для каждого администратора в таблице доступна 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 на значок **Фильтр** над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Имя**, **Электронная почта** или **Статус**:
   - Установите флажки напротив интересующих вас значений.

   Если вы выбрали параметр **Дата создания**:
   - Нажмите на интересующие вас даты. Чтобы задать период времени, нажмите на 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 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. На открывшейся странице выберите вкладку **Администраторы**.
3. Нажмите кнопку , чтобы создать администратора.

4. Во всплывающем окне **Новый администратор** укажите данные администратора: имя, адрес электронной почты и пароль (см. Рисунок 3).
5. Нажмите кнопку **Создать**.

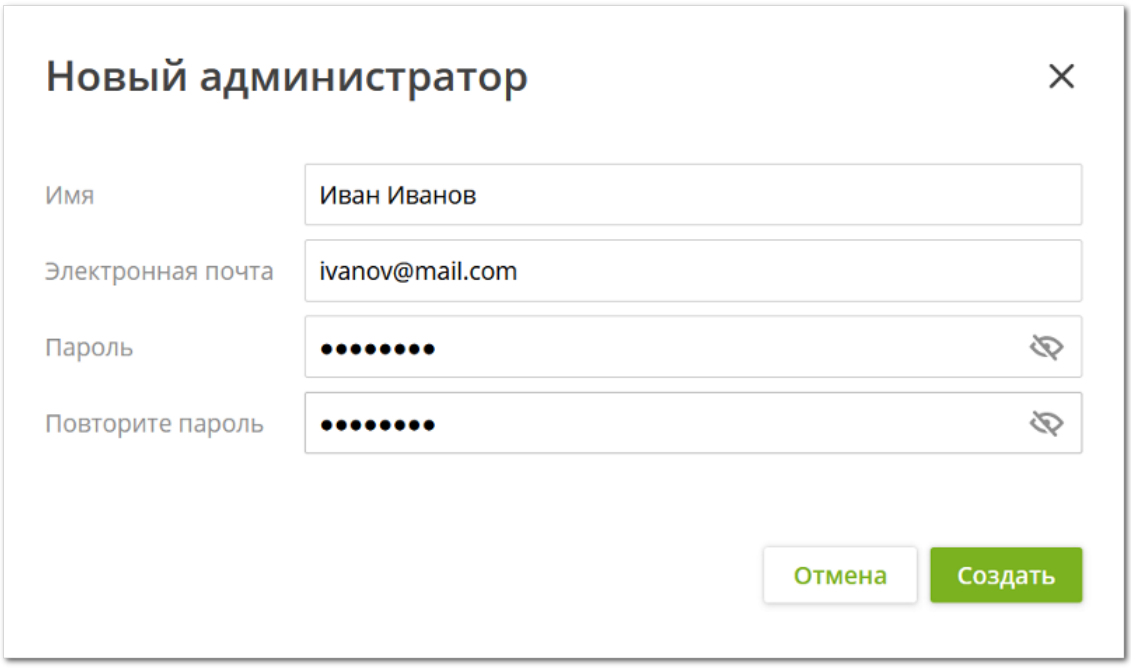

Рисунок 3. Создание нового администратора

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. Наведите курсор на строку администратора и нажмите в правой части строки.
2. Во всплывающем окне **Информация об администраторе** внесите необходимые изменения.
3. Нажмите кнопку **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 напротив пункта **Статус** на 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. Наведите курсор на строку администратора и нажмите  в правой части строки.
2. Подтвердите удаление.

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

7. Настройки Dr.Web

Вкладка **Настройки Dr.Web** находится на верхней панели веб-сервиса между вкладками **Управление** и **Фильтры**. 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;
- **Действия** — при наведении курсора на строку с настройкой в этой графе отображаются возможные действия для этой настройки (редактировать, удалить).

> Настройки не добавляются автоматически. Каждую настройку администратор добавляет вручную, указывая для нее всю необходимую информацию.

Чтобы добавить настройку:

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

> Кнопка **Сохранить** будет недоступна, пока вы не заполните все обязательные поля. Обязательными являются все поля, кроме поля **Описание**.

Чтобы изменить настройку:

1. Наведите курсор на настройку в таблице.
2. Нажмите значок , который появится в графе **Действия**.
3. Введите новые сведения в открывшемся окне **Изменение настройки**.
4. Нажмите **Сохранить**.

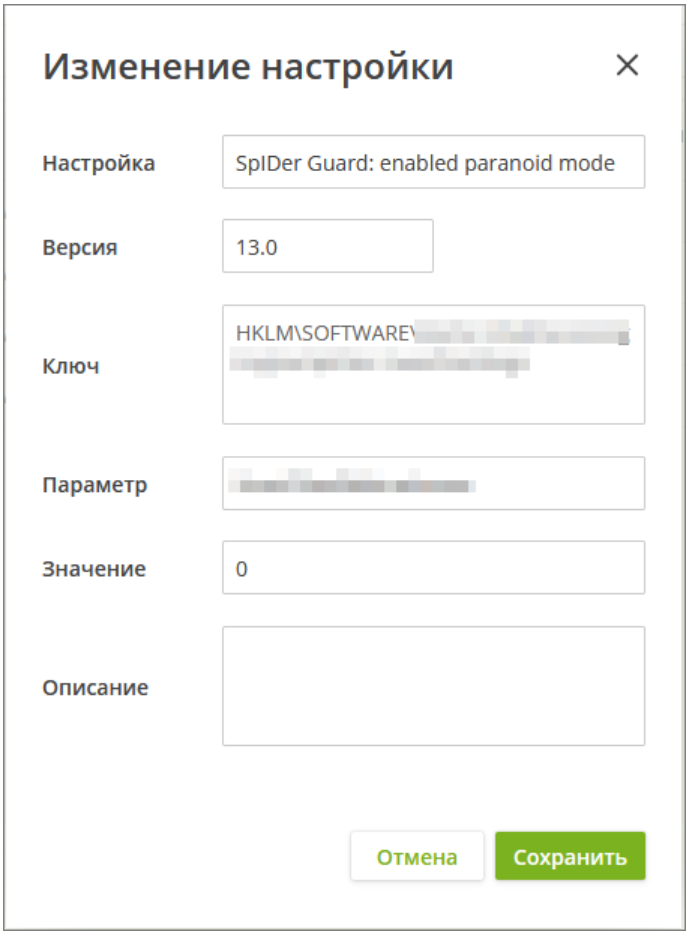

Рисунок 4. Изменение настройки.

Чтобы удалить настройку:

1. Наведите курсор на настройку в таблице.
2. Нажмите значок , который появится в графе **Действия**.
3. Подтвердите удаление в открывшемся окне **Удаление настройки**, нажав **Удалить**.

8. Фильтры

Вкладка **Фильтры** находится на верхней панели веб-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 интересует пользователя. Раздел **Фильтры** служит для того, чтобы просматривать, создавать и редактировать фильтры и группы фильтров, не выполняя при этом анализ данных конкретного отчета (см. Рисунок 5).

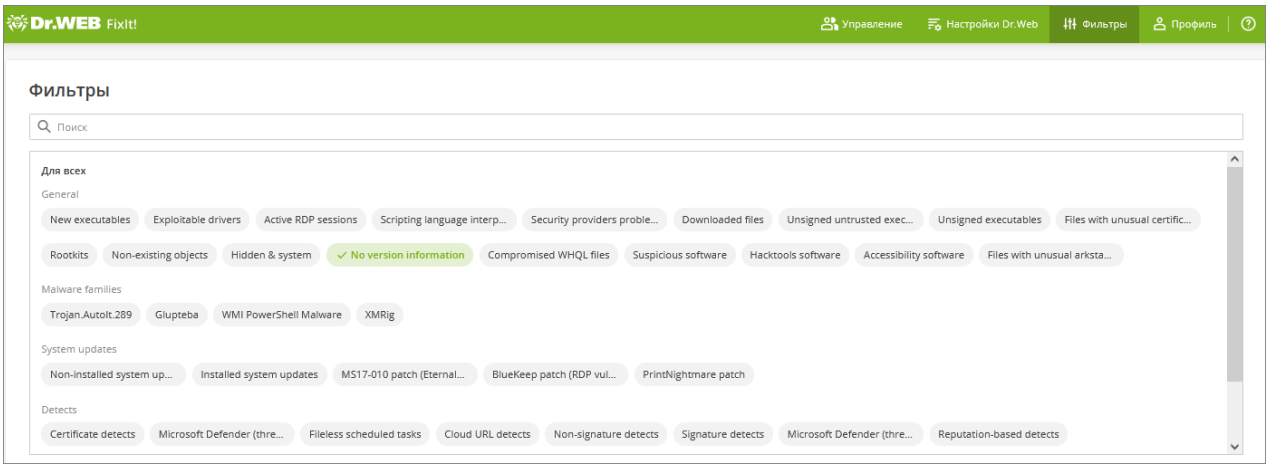

Рисунок 5. Фильтры

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 подробную информацию о запросах и полях читайте 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. Заполните поля **Имя** и **Описание**.
3. В поле **Доступен** укажите, кому будет доступен фильтр.
4. Выберите группу или создайте новую, нажав + **Новая группа**.
5. Нажмите **Сохранить как новый фильтр**.

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

Чтобы редактировать фильтр

1. Выберите фильтр из списка.
2. Внесите изменения в соответствующие поля (см. Рисунок 6).
3. При необходимости измените доступность фильтра в поле **Доступен**.
4. Выберите группу или создайте новую, нажав + **Новая группа**.
5. Нажмите **Сохранить**, чтобы применить изменения. Чтобы создать новый фильтр, нажмите **Сохранить как новый фильтр**.

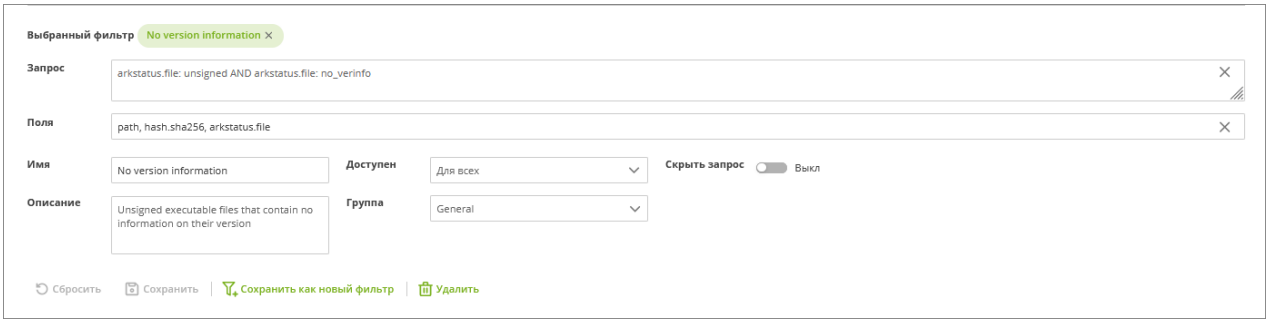

Рисунок 6. Редактирование фильтра

Чтобы удалить фильтр

1. Выберите фильтр из списка.
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**.

Вкладка **Фильтры** также служит для того, чтобы переименовывать и удалять группы фильтров.

Чтобы переименовать группу

1. Наведите курсор на имя группы, которую необходимо переименовать.
2. Нажмите  рядом с именем группы.
3. Во всплывающем окне **Редактировать группу** укажите новое имя.
4. Нажмите **Сохранить**.

Опция недоступна для группы **No group**.

Чтобы удалить группу

1. Наведите курсор на имя группы, которую необходимо удалить.
2. Нажмите  рядом с именем группы.
3. Подтвердите удаление во всплывающем окне **Удалить группу**.

При удалении группы удаляются также содержащиеся в ней фильтры. Удаленная группа фильтров не может быть восстановлена.

Опция недоступна для группы **No group**.

9. 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 на кнопку **Заметка**, чтобы добавить описание.

Нажмите **Меню** справа от описания пространства и выберите соответствующую опцию, чтобы редактировать или удалить описание.

Изменять имя, срок действия задач, лимит задач пространства и блокировать его 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 на значок  **Фильтр** над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Имя**, **Электронная почта** или **Статус**:
   - Установите флажки напротив интересующих вас значений.

   Если вы выбрали параметр **Дата создания**:
   - Нажмите на интересующие вас даты. Чтобы задать период времени, нажмите на 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 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. Во всплывающем окне **Новый пользователь** укажите данные участника: роль (Менеджер или Пользователь), имя, адрес электронной почты и пароль.
3. Нажмите кнопку **Создать**.

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.

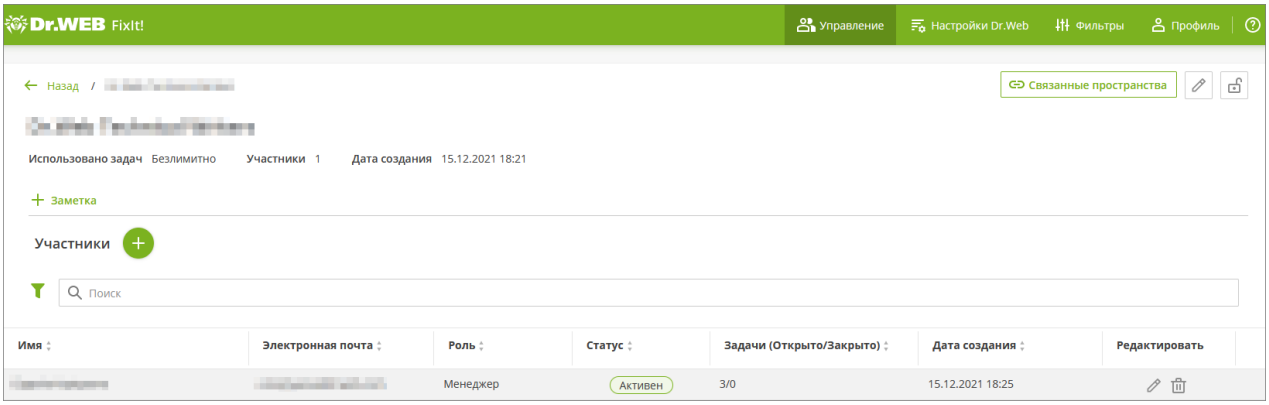

Рисунок 7. Редактирование информации об участнике

Чтобы редактировать учетную запись участника

1. Наведите курсор на строку участника и нажмите в правой части строки (см. Рисунок 7).
2. Во всплывающем окне **Информация о пользователе** внесите необходимые изменения.
3. Нажмите кнопку **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 напротив пункта **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. Наведите курсор на строку участника и нажмите в правой части строки.
2. Подтвердите удаление.

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 на кнопку **Связанные пространства** на странице пространства.

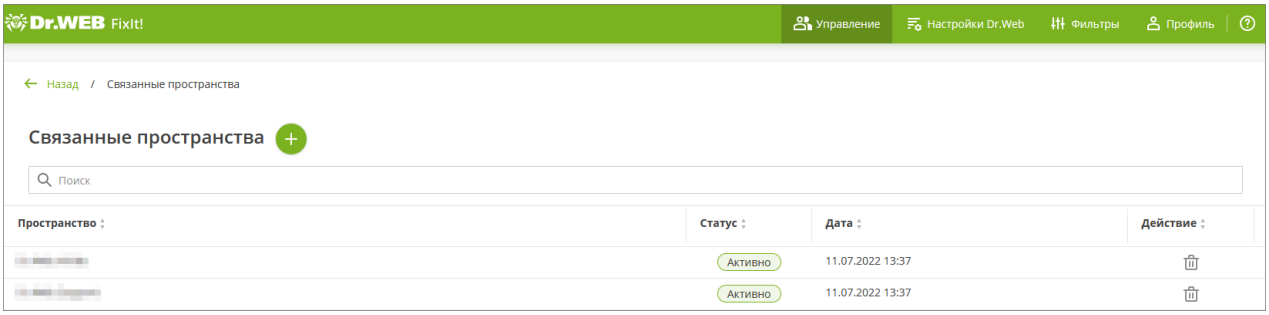

Рисунок 8. Связанные пространства

Чтобы добавить связанное пространство

1. Нажмите  рядом с заголовком страницы.
2. В открывшемся окне **Добавить пространство** найдите пространство, с которым вы хотите установить связь, и отметьте его флажком.
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.

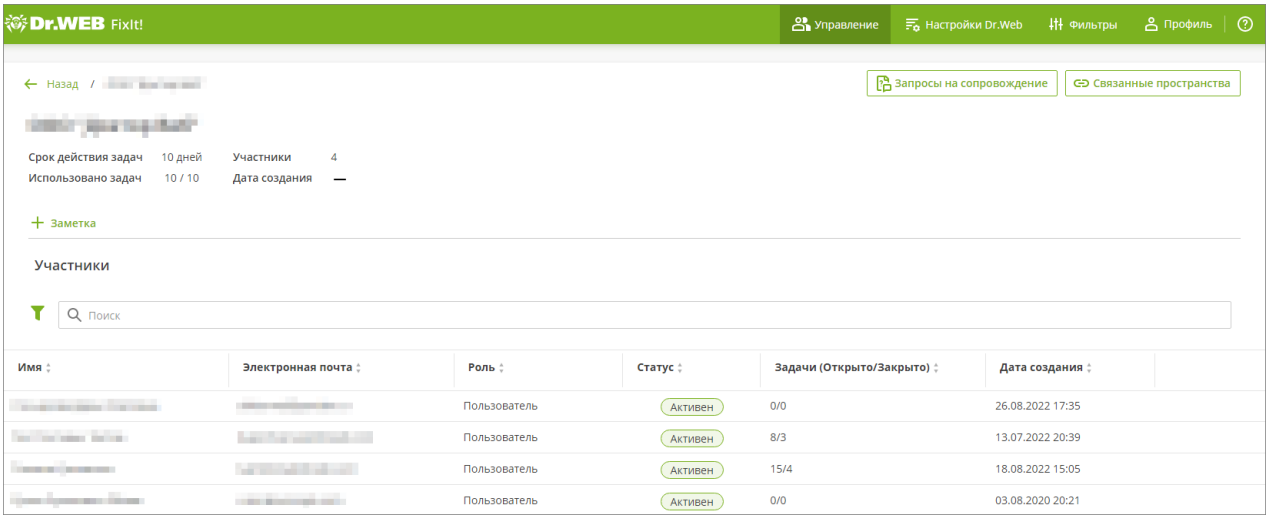

Рисунок 9. Кнопка Запросы на сопровождение.

10. 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. Для перехода к главной странице сервиса нажмите 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 или пользователя). В зависимости от роли участника доступны следующие данные:

- **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).
- **Использовано задач**: количество уже использованных задач из установленного лимита, если лимит задан (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**;
- **создатель**;
- **пространство** (доступно только для администраторов);
- **статус**: Открыта или Закрыта;

- **отчеты**: количество отчетов, полученных в рамках задачи;
- **дата создания**;
- **последнее изменение**.

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

Создайте новую или выберите существующую задачу для начала или продолжения работы в сервисе.

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 на 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 на значок  **Фильтр** над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Создатель**, **Пространство** или **Статус**:
   - Установите флажки напротив интересующих вас значений.

   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.
4. Нажмите кнопку **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 задач

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.

10.1. 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 (см. Рисунок 10) доступна следующая информация:

- имя задачи,
- срок действия,
- создатель,
- дата создания,
- отчеты,
- источник,
- последнее изменение,
- описание задачи.

Описание задачи может добавить или редактировать администратор или любой участник пространства. Нажмите на кнопку + **Заметка**, чтобы добавить описание.

Нажмите ⋮ **Меню** справа от описания задачи и выберите соответствующую опцию, чтобы редактировать или удалить описание.

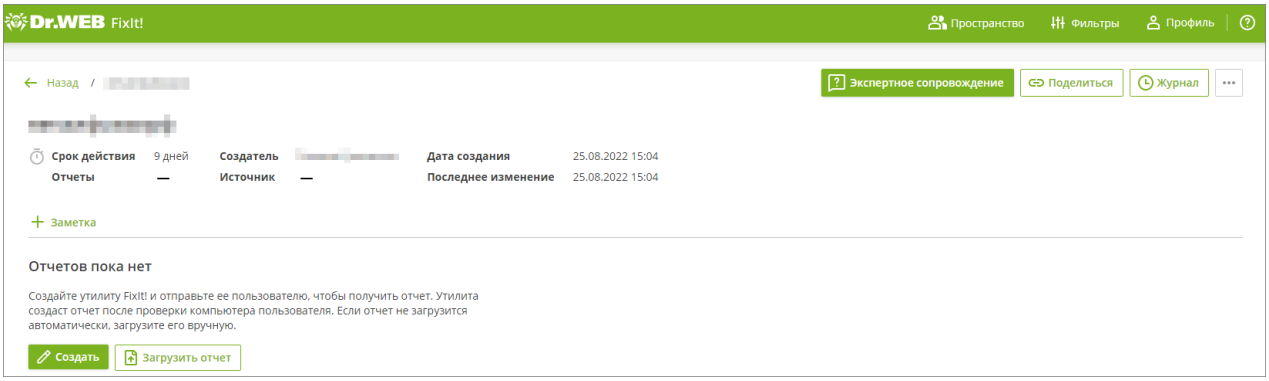

Рисунок 10. Задача

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 в появившемся меню нажмите **Переименовать**.
- Наведите курсор на имя задачи и нажмите на появившийся значок .

2. Введите новое имя задачи.

Изменения сохранятся автоматически.

Чтобы закрыть задачу

1. В правом верхнем углу страницы задачи нажмите ...
2. В появившемся меню нажмите **Закрыть задачу**.
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 ...
2. В появившемся меню нажмите **Удалить**.
3. Подтвердите удаление задачи.

Открытие доступа к задаче

Задачами можно делиться со связанными пространствами для совместной работы. Делиться задачами могут как администраторы, так и менеджеры и пользователи.

Чтобы поделиться задачей

1. Нажмите кнопку **Поделиться** в правом верхнем углу страницы задачи.
2. На открывшейся странице **Поделиться** нажмите .
3. В открывшемся окне **Добавить пространство** отметьте флажком 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 графе **Источник**.

Чтобы закрыть доступ к задаче

1. Нажмите кнопку **Поделиться** в правом верхнем углу страницы задачи.
2. На открывшейся странице **Поделиться** наведите курсор на строку с пространством, которому вы хотите закрыть доступ к задаче, и нажмите в графе **Действие**.
3. Подтвердите удаление в открывшемся окне.

Страница Поделиться

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

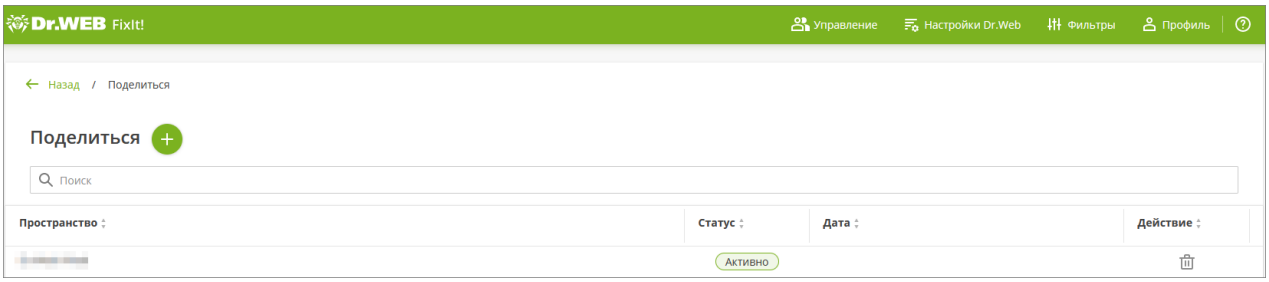

Рисунок 11. Страница Поделиться

В таблице сведений о пространствах, имеющих доступ к задаче, содержится следующая информация (см. Рисунок 11):

- 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 Сбор информации утилитой FixIt!).

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).

10.2. Сбор информации утилитой FixIt!

Утилита FixIt! собирает данные о системе и формирует детальный отчет.

Для получения первого отчета в рамках задачи необходимо создать анализирующую утилиту FixIt!. После получения отчета и анализа полученных данных в утилиту FixIt! можно добавить лечащие команды для устранения проблем и обезвреживания угроз на проверяемом компьютере (см. раздел Команды утилиты).

Настройки утилиты FixIt!

При создании утилиты FixIt! для сбора данных вам предлагается ее настроить (см. Рисунок 12).

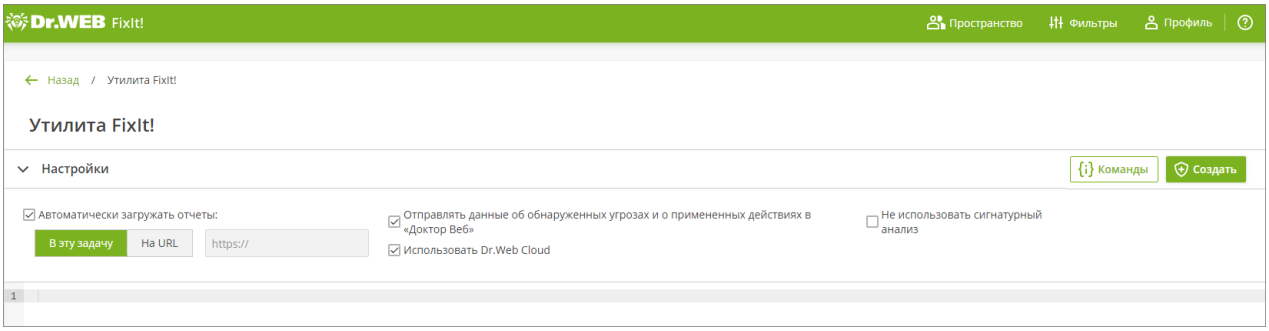

Рисунок 12. Настройки утилиты FixIt!

Команды анализирующей утилиты FixIt!

Вы можете добавить команды для сбора информации об интересующих вас элементах системы в утилиту FixIt! вручную (см. раздел Команды сбора информации).

Поле для ввода команд расположено на странице создания утилиты FixIt! под выпадающим меню **Настройки**. Чтобы просмотреть список доступных команд, нажмите кнопку **Команды** в правой части меню **Настройки**.

Чтобы создать анализирующую утилиту FixIt!

- Если в нужной задаче нет загруженных отчетов:
  1. Зайдите в нужную задачу.
  2. Нажмите кнопку **Создать**.
  3. Задайте необходимые настройки в выпадающем меню **Настройки**.
  4. При необходимости введите команды в поле под выпадающим меню **Настройки**.
  5. Нажмите кнопку **Создать**.
- Если в нужной задаче уже есть загруженные отчеты:
  1. Зайдите в нужную задачу.
  2. Откройте любой отчет из списка.
  3. В меню слева перейдите в раздел **Утилита FixIt!**.
  4. Задайте необходимые настройки в выпадающем меню **Настройки**.
  5. При необходимости введите команды в поле под выпадающим меню **Настройки**.
  6. Нажмите кнопку **Создать**.

После создания утилиты на экране появится всплывающее окно, позволяющее выбрать способ отправки утилиты владельцу проверяемого компьютера (см. Рисунок 13).

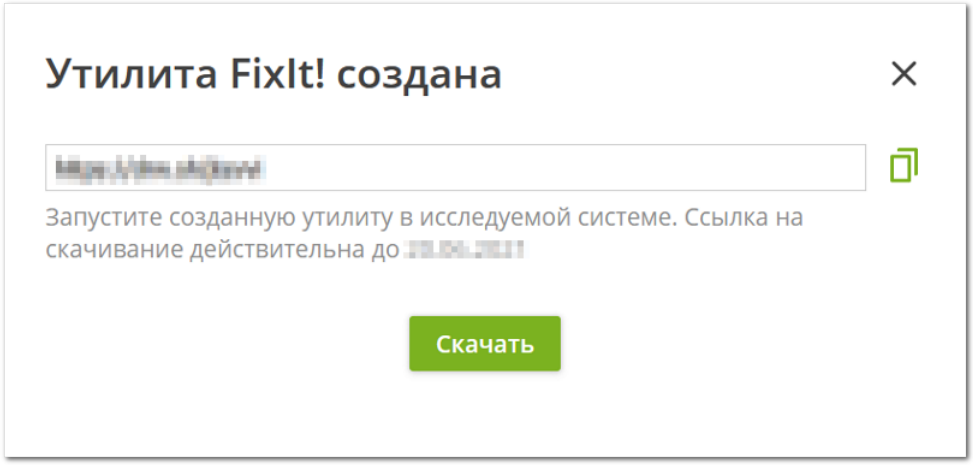

Рисунок 13. Утилита создана

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

Для сбора информации о системе пользователю необходимо запустить утилиту на проверяемом компьютере и отправить созданный утилитой отчет.

10.3. Отчет

Отчет содержит подробную информацию о состоянии системы проверяемого компьютера на момент запуска утилиты FixIt!.

Загрузка отчета

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

Чтобы загрузить отчет автоматически, установите флажок **Автоматически загружать отчеты** при сборке утилиты (более подробная информация о сборке приведена в разделе Проверка компьютера утилитой).

Чтобы загрузить отчет вручную

- Если в нужной задаче нет загруженных отчетов:
  1. Зайдите в нужную задачу.
  2. Нажмите кнопку **Загрузить отчет**.

3. Перетащите архив с отчетом на область загрузки в открывшемся окне или нажмите **Выберите** и выберите архив в проводнике.
4. Нажмите кнопку **Загрузить**.

- Если в нужной задаче уже есть загруженные отчеты:
  1. Зайдите в нужную задачу.
  2. Нажмите кнопку  под заголовком **Отчеты**.
  3. Перетащите архив с отчетом на область загрузки в открывшемся окне или нажмите **Выберите** и выберите архив в проводнике.
  4. Нажмите кнопку **Загрузить**.

После загрузки в задачу отчет автоматически анализируется, а его данные группируются в категории (см. раздел Данные). При необходимости вы можете запустить повторный анализ отчета, нажав значок  в списке отчетов.

Таблица Отчеты

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 на значок  **Фильтр** над таблицей.
2. Выберите параметр фильтрации.

3. Если вы выбрали параметр **Способ загрузки**:
   - Установите флажки напротив интересующих вас значений.

   Если вы выбрали параметр **Дата загрузки**:
   - Нажмите на интересующие вас даты. Чтобы задать период времени, нажмите на 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 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.

Просмотр отчета

Для просмотра и дальнейшей работы с отчетом нажмите на имя отчета в таблице отчетов (см. раздел Отчеты).

10.4. 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:

- **дата**,
- **действие**,
- **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 отчета.
- Действия с фильтрами:
  - удаление,
  - изменение,
  - добавление,
  - сохранение.
- Ошибка распознавания файла — текст ошибки выводится во всплывающем окне.
- Создание утилиты 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.

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 на значок **Фильтр** над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Источник/Инициатор** или **Действие**:
   - Установите флажки напротив интересующих вас значений.

   Если вы выбрали параметр **Дата**:
   - Нажмите на интересующие вас даты. Чтобы задать период времени, нажмите на 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 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, нажмите кнопку **Обновить** на странице журнала.

Чтобы скачать журнал, нажмите значок на странице журнала. Журнал сохраняется в виде файла с расширением .log. Открыть файл можно с помощью любого текстового редактора.

10.5. 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. Нажмите кнопку **Экспертное сопровождение** вверху страницы.
3. В открывшемся окне укажите серийный номер сертификата на экспертное сопровождение задачи (см. Рисунок 14). Данные должны быть 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 кнопку **Купить у партнеров**, чтобы приобрести сертификат у партнеров компании «Доктор Веб».
   - Нажмите кнопку **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.

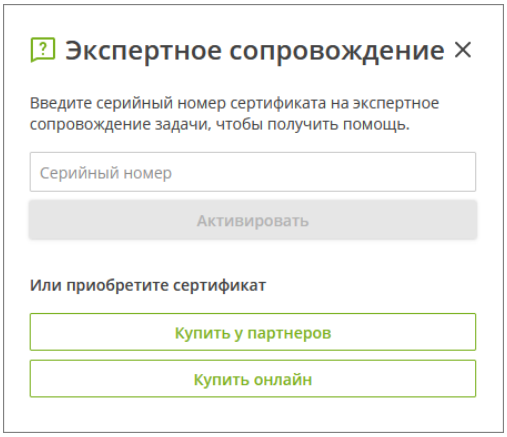

Рисунок 14. Запрос экспертного сопровождения.

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 получите уведомления на электронную почту о любых изменениях в статусе вашего запроса, а также о появлении ответов на него.

Для перехода на страницу существующего запроса

1. Перейдите на страницу соответствующей задачи.
2. Нажмите кнопку **Экспертное сопровождение** вверху страницы.

ИЛИ

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

ИЛИ

1. Перейдите на страницу пространства.
2. Нажмите кнопку **Запросы на сопровождение** вверху страницы.
3. На открывшейся странице выберите нужный запрос из списка (см. Рисунок 15).
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. Нажмите кнопку **Запросы на сопровождение** вверху страницы.

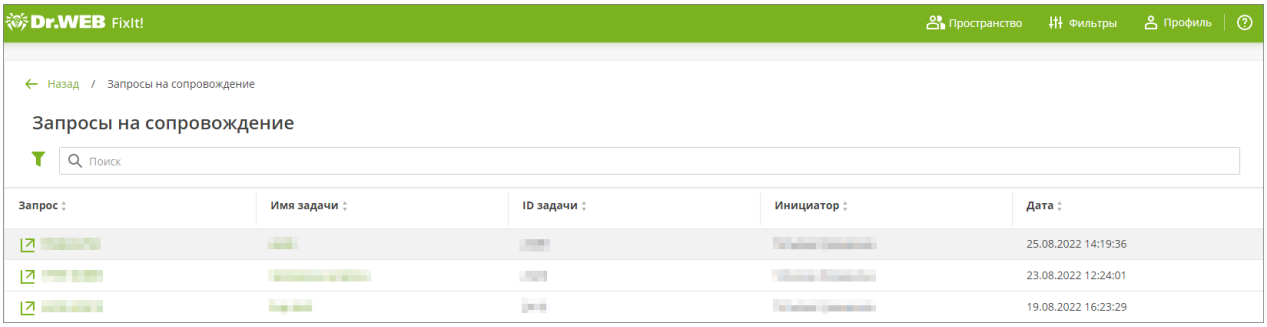

Рисунок 15. Список запросов на сопровождение.

В таблице запросов на сопровождение отображается следующая информация:

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

11. Отчеты

Отчеты содержат детальную информацию, собранную утилитой FixIt! на проверяемом компьютере.

Как работать с отчетами

- Чтобы ознакомиться с отчетом, загрузите его в нужную задачу.
- Чтобы проанализировать данные, используйте фильтры и сравнивайте отчеты, созданные в разное время.
- Чтобы нейтрализовать обнаруженные угрозы, создайте лечащую утилиту FixIt!.

При открытии отчета на левой боковой панели доступны вкладки, позволяющие:

- просматривать общую информацию об отчете,
- просматривать все данные отчета по категориям,
- выполнять поиск по отчету и анализировать данные отчета с помощью фильтров,
- создавать утилиту FixIt! для дальнейшего анализа и лечения системы проверяемого компьютера,
- просматривать и скачивать собранные утилитой файлы с проверяемого компьютера.

11.1. Об отчете

Вкладка **Об отчете** открывается при нажатии имени отчета на странице задачи. На вкладке **Об отчете** вы можете:

- просмотреть общую информацию о файле отчета,
- переименовать отчет,
- скачать отчет,
- сравнить текущий отчет с любым другим отчетом из этой же задачи.

11.1.1. Общая информация об отчете

Вкладка **Об отчете** содержит следующую информацию о файле отчета:

- **Способ загрузки**: Вручную или Автоматически.
- **Дата создания**: дата формирования отчета.
- **Размер, МБ**: размер файла отчета в мегабайтах.
- **Ключ**: пароль от ZIP-архива с отчетом. Ключ можно скопировать, нажав на него.
- **Имя устройства**: имя устройства, при проверке которого был создан отчет.
- **Заметка**: описание отчета.

Описание отчета может добавить или редактировать администратор или любой участник пространства. Нажмите на кнопку + **Заметка**, чтобы добавить описание.

Нажмите ⋮ **Меню** справа от описания отчета и выберите соответствующую опцию, чтобы редактировать или удалить описание.

Редактирование отчетов

Все участники сервиса могут переименовывать отчеты в любых доступных им задачах. Администраторы и менеджеры также могут удалять отчеты.

Чтобы переименовать отчет

1. Выполните одно из следующих действий:
   - В правом верхнем углу вкладки **Об отчете** нажмите ··· и в появившемся меню нажмите **Переименовать**.
   - Наведите курсор на имя отчета и нажмите на появившийся значок ✎
2. Введите новое имя отчета.

Изменения сохранятся автоматически.

Чтобы удалить отчет

1. Нажмите значок ··· в правом верхнем углу вкладки **Об отчете**.
2. Нажмите 🗑 **Удалить**.
3. Во всплывающем окне подтвердите удаление.

Скачивание отчета

Любой участник сервиса может сохранить отчет из доступной ему задачи локально на свой компьютер.

Чтобы скачать отчет

1. Нажмите значок ··· в правом верхнем углу вкладки **Об отчете**.
2. Нажмите ⤓ **Скачать**.

Скачивание начнется автоматически. Файл отчета будет сохранен на ваш компьютер в формате .zip.

11.1.2. Сравнение отчетов

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. Нажмите кнопку **Сравнить** в правом верхнем углу вкладки **Об отчете**.
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** (см. Рисунок 16) 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.

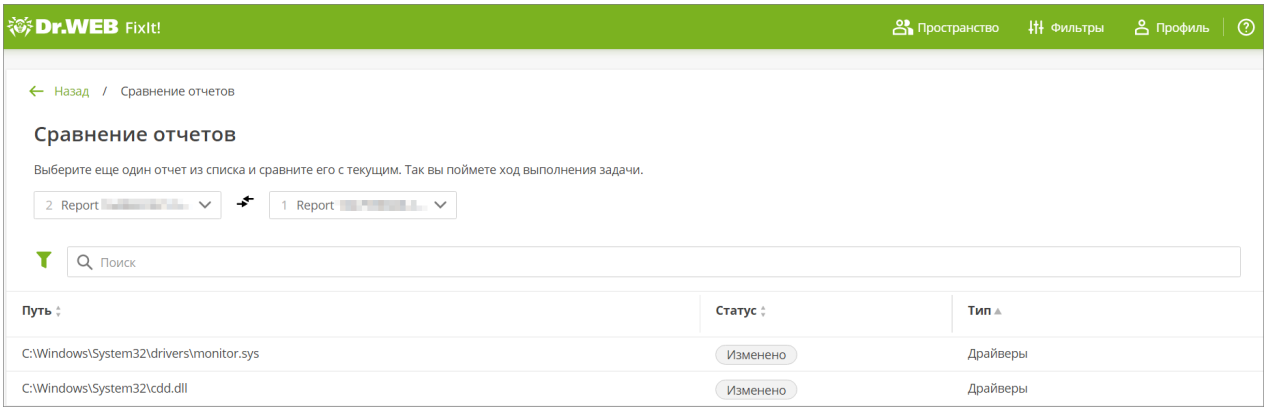

Рисунок 16. Сравнение отчетов

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 на значок **Фильтр** над таблицей.
2. Выберите параметр фильтрации.
3. Установите флажки напротив интересующих вас значений.
4. Нажмите кнопку **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.

11.2. Данные

Вкладка **Данные** содержит все данные, вошедшие в отчет. Данные распределены по категориям:

- Dr.Web,
- Система,
- 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.

Данные представлены в виде выпадающего меню. Нажмите на вкладку **Данные**, чтобы развернуть или свернуть список.

11.2.1. Dr.Web

В раздел Dr.Web загружается сводка информации об установленном на устройстве продукте компании «Доктор Веб». В разделе две вкладки: на вкладке **Общие** слева указаны общие сведения, а на вкладке **Измененные настройки** справа указаны отличия текущих настроек продукта от настроек по умолчанию.

Информация на вкладке **Общие** делится 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,
- **хэш**: хэш-сумма файла программы,
- **путь**: расположение папки с файлами программы,
- **репозиторий**: расположение репозитория,
- **путь к базам**: расположение 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 графе **Статус** появляется значок галочки.

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 значок >.

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,
- **выявляемые 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,
- расположение,
- скрипт удаления.

11.2.2. Система

Вкладка **Система** содержит данные о системе проверяемого компьютера.

Данные распределены по категориям и представлены в виде сворачивающихся блоков.

Категория	Параметры
Процессоры	• имя, • описание, • базовая частота, ГГц, • максимальная частота, ГГц, • физические процессоры, • логические процессоры.

Категория	Параметры
Оперативная память	• локальная, МБ, • виртуальная, МБ.
ОС	• имя, • версия, • сборка, • тип системы, • режим загрузки, • папка, • время работы, • местное время.
Локализация	• часовой пояс, • страна или регион, • язык ОС, • язык интерфейса.
Жесткие диски	• диск, • серийный номер, • свободное место, ГБ, • файловая система, • метка.
Учетные записи	• имя, • описание, • скрипт, • тип, • группы.
Сетевой диск	• имя пользователя, • удаленный каталог, • имя провайдера, • буква диска.
Ярлык сетевого ресурса	• имя пользователя, • имя, • путь.
Переменная среды	• описание, • путь.
Антивирус и брандмауэр	• компания, • версия, • продукт, • включены.

Категория	Параметры
Индекс производительности	• оперативная память, • процессоры, • 3D-графика, • графика, • диск, • средний балл.

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

11.2.3. 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 MSI	• имя, • версия, • разработчик.
Приложения из магазина Microsoft Store	• имя, • версия, • ID.

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.

11.2.4. 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 на его имя. В правой части экрана появится всплывающее окно **Подробности** со сведениями о параметрах объекта:

Вкладка	Доступные параметры
Процесс	• Статус • Свойства: ▪ PID ▪ Сессия ▪ Адрес ▪ Путь ▪ Командная строка ▪ Текущий каталог ▪ Разрядность ▪ Адрес PEB ▪ Запуск под отладчиком ▪ Уровень изоляции ▪ Дата создания • Ресурсы: ▪ Kernel time ▪ User time ▪ Приоритет ▪ Handles • Родитель
Файл	• Путь • Статус: ▪ Сертификат ▪ Файл ▪ Тип ▪ Облако

Вкладка	Доступные параметры
	▪ Тип ПО • Хэш: ▪ SHA1 ▪ SHA256 ▪ Ссылка на сервис VirusTotal • Свойства: ▪ Размер ▪ Дата создания ▪ Последнее изменение ▪ 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 создания

11.2.5. 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 на путь к файлу драйвера в таблице. Доступна следующая информация о драйверах:

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

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

Вкладка	Доступные параметры
	▪ тип, ▪ облако, ▪ тип ПО; • хэш: ▪ 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.

11.2.6. 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 на 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.

Вкладка	Доступные параметры
Файл	• путь; • статус: ▪ сертификат, ▪ файл, ▪ тип, ▪ облако, ▪ тип ПО; • хэш: ▪ 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.

11.2.7. 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, • 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.

Вкладка	Параметры
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.

11.2.8. 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,

Вкладка	Данные
	▪ путь, ▪ компания, ▪ подписан, ▪ репутация; • локальные провайдеры имен Winsock: ▪ имя, ▪ запуск, ▪ путь, ▪ компания, ▪ подписан, ▪ репутация.
Автозагрузки через реестр	Вкладка содержит список автозагрузок. По нажатию на строку автозагрузки разворачивается таблица со следующей информацией об автозагрузке: • ключ, • путь, • компания, • подписан, • репутация.
Ярлыки	Вкладка содержит список ярлыков в системе. По нажатию на строку 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, • 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; • хэш: ▪ SHA1, ▪ SHA256; ▪ ссылка на сервис VirusTotal; • свойства: ▪ размер, ▪ дата создания, ▪ последнее изменение,

Вкладка	Доступные параметры
	▪ 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.

11.2.9. 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.

11.2.10. 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 на ID нужного расширения; данные о настройках можно получить, нажав на 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.

11.2.11. 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 значок ›, 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 на значок **Фильтр** над таблицей.
2. Выберите параметр фильтрации.
3. Если вы выбрали параметр **Источник**, **Файл** или **Компьютер**:
   - Установите флажки напротив интересующих вас значений.

   Если вы выбрали параметр **Дата**:
   - Нажмите на интересующие вас даты. Чтобы задать период времени, нажмите на 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.

11.2.12. 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 на 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 на ключ реестра в списке или на 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.

11.2.13. 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 на вкладку **Дерево**.

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

- **имя**: путь к файлу,
- **SHA1**: хэш-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 на путь к файлу в таблице на вкладке **Список** или на 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; • хэш: ▪ 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.

11.3. Файлы

Файлы, собранные в процессе проверки компьютера утилитой FixIt!, отображаются в разделе **Файлы** в виде таблицы:

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 .

При возникновении ошибки в ходе проверки файла появляется 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, нажмите значок  .
- Чтобы скачать несколько файлов сразу, установите флажки рядом с нужными файлами и нажмите кнопку **Скачать**.

12. 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.

12.1. Готовые фильтры

На вкладке **Готовые фильтры** находятся предустановленные фильтры, в которых уже задан поисковый запрос по определенным параметрам.

Предустановленные фильтры — это фильтры по умолчанию, а также фильтры, созданные участниками пространства.

Чтобы выбрать предустановленный фильтр

1. Нажмите ⌄ в правой части панели на вкладке **Готовые фильтры**.
2. Установите флажки напротив необходимых фильтров.

Наведите курсор на значок ⓘ справа от фильтра, чтобы увидеть описание фильтра.

Фильтры распределены по категориям:

- **Для текущей задачи** — доступны в пределах выбранной задачи.
- **Для всех** — доступны всем участникам сервиса.
- **Для меня** — доступны в пределах вашего профиля.
- **Для этого пространства** — доступны в пределах выбранного пространства.

Внутри категории фильтры объединены в группы (см. Группы фильтров).

Для поиска определенного фильтра воспользуйтесь строкой глобального поиска, расположенной в верхней части выпадающего списка предустановленных фильтров. Фильтры, которые уже использовались в процессе работы с отчетом, отображаются над строкой глобального поиска.

Результаты поиска по фильтру

Данные отчета, соответствующие установленным фильтрам, отображаются ниже панели выбора фильтров в виде сворачивающихся блоков, содержащих списки найденных объектов. Каждый список соответствует одному фильтру. Если данных, соответствующих фильтру, найдено не было, то список не отображается.

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

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

Остальные столбцы таблицы представляют собой поля, заданные в фильтре.

Действия

Для каждого найденного по фильтру 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.

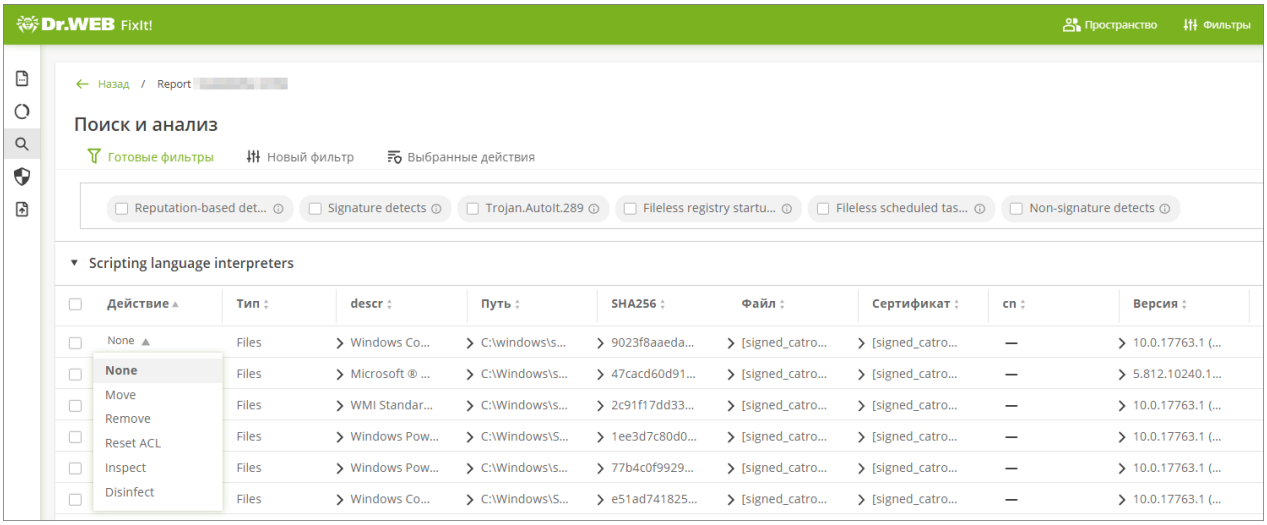

Рисунок 17. Выбор действия для файла

Доступные действия перечислены в виде выпадающего списка в столбце **Действие** в таблице результатов поиска по фильтру (см. Рисунок 17).

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 (см. Рисунок 18).

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.

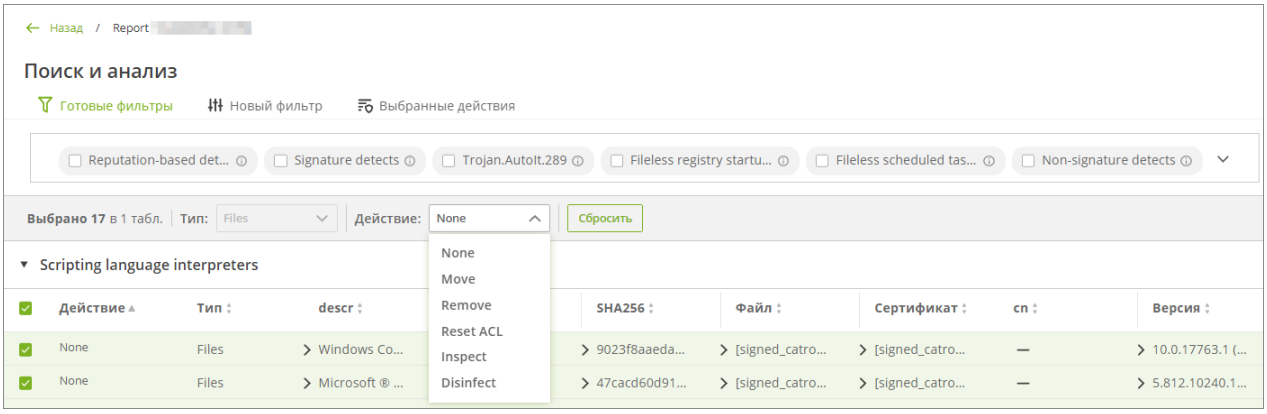

Рисунок 18. Выбор группового действия

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, Chromium 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

Действие	Описание	Тип объекта
Disinfect	Вылечить объект	Files, Registry startups, Registry, Non-signature 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.

12.2. Новый фильтр

На вкладке **Новый фильтр** вы можете создать новый фильтр, в том числе на основе предустановленного. Вкладка позволяет:

- создавать новые фильтры,
- редактировать фильтры,

- удалять фильтры,
- создавать новую группу 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).
- **Поле.** 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 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.
- **Для текущей задачи.** Опция доступна всем участникам сервиса. Фильтр будет виден всем пользователям, работающим с этой задачей.

Создание нового фильтра

Создать новый фильтр может любой участник сервиса.

Чтобы создать фильтр

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

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

2. Заполните **Поля**.
3. Нажмите **Сохранить как новый фильтр**.
4. Заполните поля **Имя** и **Описание**.
5. В поле **Доступен** укажите, кому будет доступен фильтр.
6. Выберите группу или создайте новую, нажав + **Новая группа** и заполнив необходимые поля.
7. Нажмите **Сохранить**.

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

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

Редактирование и удаление фильтра

Редактировать и удалять глобальные фильтры могут только администраторы. Редактировать и удалять фильтры текущего пространства, фильтры задачи и личные фильтры может любой участник сервиса.

Чтобы редактировать фильтр

1. На вкладке **Новый фильтр** нажмите + **Мои фильтры**.

2. Выберите фильтр.
3. Измените необходимые параметры фильтра.
4. Если вы хотите сохранить изменения в выбранном фильтре:
   - Нажмите **Сохранить изменения**.
   - Подтвердите действие во всплывающем окне.

После сохранения вы необратимо измените фильтр для всех участников 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 **Мои фильтры**.
2. Выберите необходимый фильтр.
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** в левом нижнем углу.

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 ВВОД прямо в поле **Запрос** или **Поля**.

12.2.1. 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*.

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

12.3. 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 на 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!.

13. Утилита FixIt!

Утилита FixIt! собирает данные о системе и формирует детальный отчет. Отчет загружается в задачу автоматически. Вы также можете загрузить отчет в задачу вручную. Кроме сбора данных утилита может обезвреживать обнаруженные угрозы.

- При создании задачи вы настраиваете утилиту FixIt! для сбора данных.
- После анализа загруженного отчета вы создаете лечащую утилиту FixIt! — утилиту, которая помимо сбора данных выполняет скрипт с заданными вами командами лечения.

13.1. 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! для сбора данных еще раз.

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 применяемых 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

Настройка	Описание
	позволяет уменьшить размер утилиты. Рекомендуется только в том случае, если на проверяемом компьютере уже установлен антивирусный продукт Dr.Web.

13.2. Команды утилиты

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 на 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.

13.2.1. Команды сбора информации

Для того чтобы получить данные о проверяемом компьютере, создайте утилиту FixIt!.

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. Ниже указаны доступные команды. Чтобы просмотреть список доступных команд в веб-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;

Команда	Описание
	• 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 символа, например, photo121209.jpg, photomama09.jpg или photo----09.jpg.
`inspect-reg` *<SID>* *<Путь к ключу>*	Собрать информацию о ключе реестра. 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.

Команда	Описание
	Пример: `inspect-drv --imagebase 0xfffff8064e540000`

13.2.2. Команды лечения

После того как вы получили 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 (см. Рисунок 19).

Рисунок 19. Создание лечащей утилиты FixIt!

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

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

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.

Команда	Описание
	Идентификатор присваивается в процессе сборки отчета. Пример: `disinfect-reg "629387a5dbc86d60842f12af5c43ffa5816140cc"`
`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`

Команда	Описание
Файловая система	
`fs-move` <*Источник*> <*Назначение*>	Переместить или переименовать файл или каталог. 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.

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.
	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. Пример: `reg-reset-acl -r HKLM SOFTWARE\Test`

Команда	Описание
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. Пример: `proc-suspend --imagename win32calc.exe`
Службы	

Команда	Описание
`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. Пример: `task-delete \Microsoft\Windows\TestTask`
Многоуровневые поставщики услуг	
`lsp-delete <GUID>`	Удалить зарегистрированные провайдеры с указанным в реестре `GUID`.

Команда	Описание
	Пример: `lsp-delete {f9eab0c0-26d4-11d0-bbbf-00aa006c34e4}`
Поставщики пространства имен	
`nsp-delete <GUID>`	Удалить зарегистрированных провайдеров с указанным в реестре `GUID`. Пример: `nsp-delete {6642243a-3ba8-4aa6-baa5-2e0bd71fdd83}`
Поставщики WMI	
`wmi-delete-eventconsumer <Пространство имен> <Имя класса> <Значение>`	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. Пример: `hosts-clear c:\Windows\System32\drivers\etc\hosts 44 45 46`
`hosts-default <Путь>`	Восстановить стандартный для системы файл HOSTS.

Команда	Описание
	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.
	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. 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. 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.

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

13.3. Проверка компьютера утилитой

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

На начальном экране утилиты (см. Рисунок 20) доступны настройки:

- **Разрешить использование Dr.Web Cloud**: доступна, если при создании утилиты был установлен флажок **Использовать Dr.Web Cloud**.
- **Отправить отчет на сервер**: доступна, если при создании утилиты был установлен флажок **Автоматически загружать отчеты**.

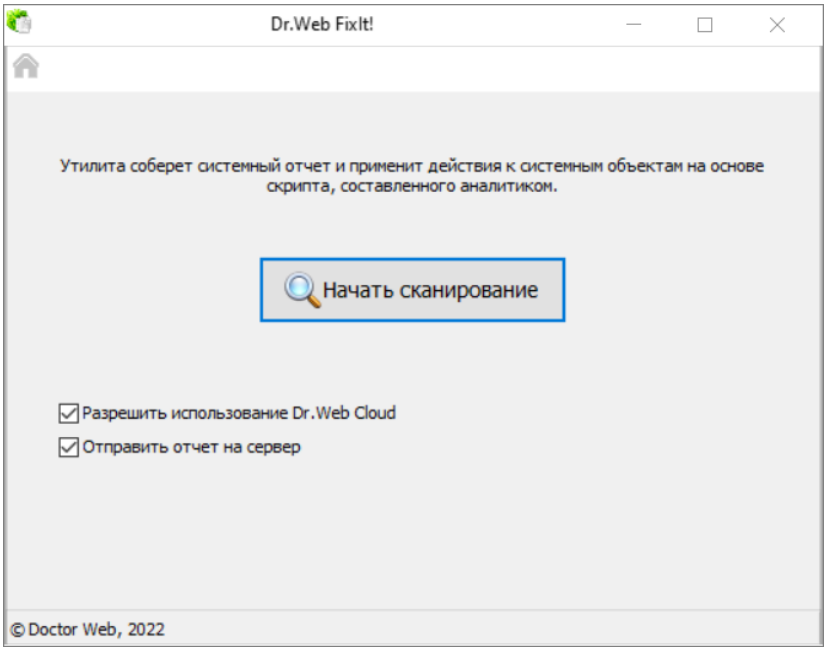

Рисунок 20. Начальный экран утилиты FixIt!

Установите необходимые настройки и нажмите кнопку **Начать сканирование**.

Утилита соберет информацию об указанных элементах.

Чтобы прервать сбор данных, нажмите **Стоп**. Прерванную операцию нельзя будет продолжить. Чтобы запустить сканирование вновь, вернитесь на начальный экран утилиты, нажав кнопку в левом верхнем углу окна, затем нажмите кнопку **Начать сканирование**.

После успешного окончания сканирования утилита создаст ZIP-архив с данными отчета в папке `C:\Users\<Пользователь>\Doctor Web`. Ссылка на файл доступна в окне утилиты после окончания проверки (см. Рисунок 21). В ту же папку сохраняется файл с расширением .zip_password, представляющий собой текстовый документ с паролем от ZIP-архива. Пароль также отобразится на странице отчета после загрузки отчета на сервис Dr.Web FixIt!.

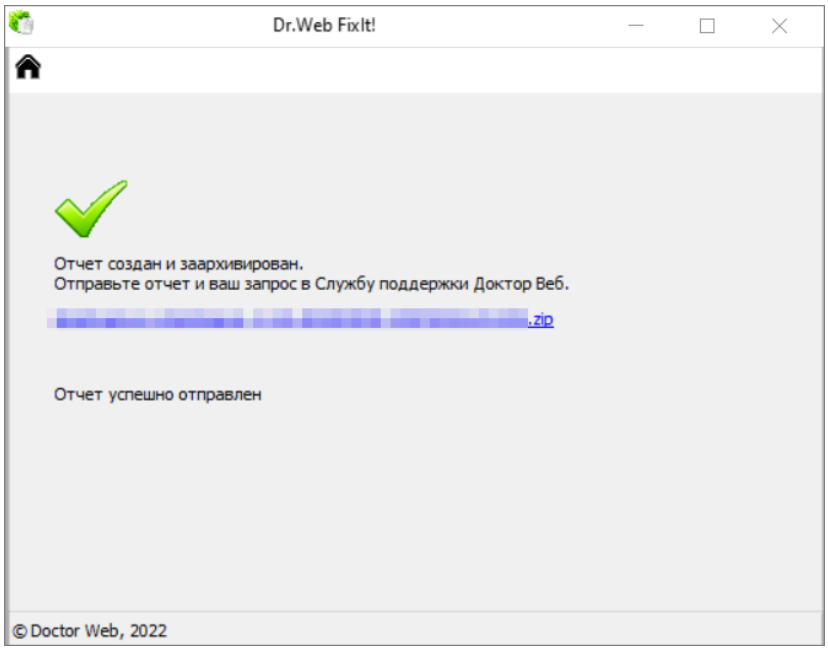

Рисунок 21. Ссылка на созданный отчет

Если при запуске сканирования был установлен флажок **Автоматически загружать отчеты**, отчет будет загружен на страницу задачи автоматически после окончания сканирования. В ином случае отчет необходимо загрузить вручную.

14. 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/.

15. Приложение А. Пример использования

Здесь мы рассмотрим пример использования веб-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 веб-сервис Dr.Web FixIt!.

Решение

Как всегда, мы начали с подготовки к работе с веб-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 следующие фильтры раздела **General**:

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

- Files with unusual certificates

и следующие фильтры раздела **Detects**:

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

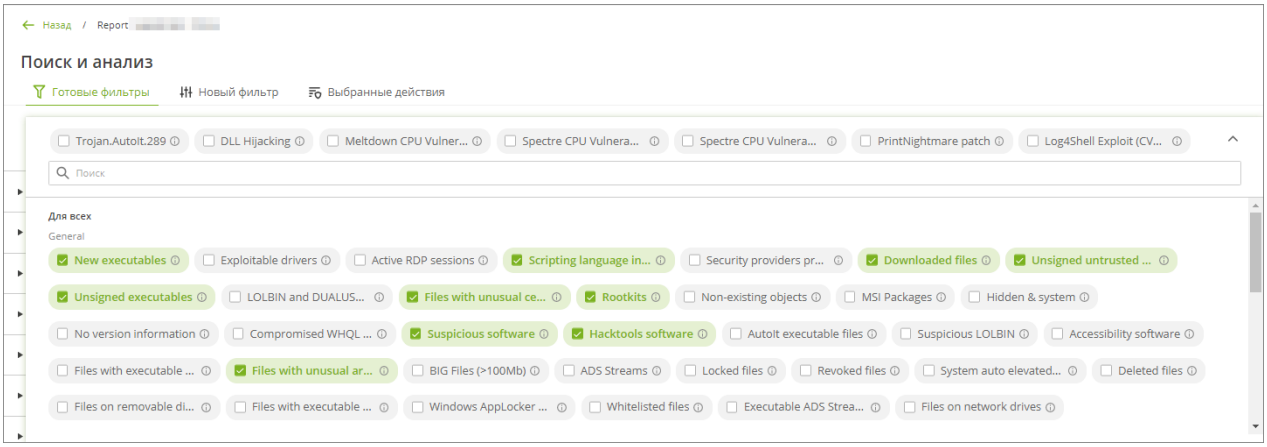

Рисунок 22. Выбранные фильтры

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.

▼ Reputation-based detects

Действие	Тип	Путь	SHA1	Результат
None	Files	C:\ProgramData\RealtekHD\taskhostw.exe	77125109b64a784b85de17a0777fe9b895737dfc	infected
None	Files	C:\programdata\windowstask\AMD.exe	b55e011feb9948301f50ae38c27cfe0f427e6ac5	infected
None	Files	C:\programdata\windowstask\AppModule.exe	b55e011feb9948301f50ae38c27cfe0f427e6ac5	infected
None	Files	C:\ProgramData\WindowsTask\MicrosoftHost.exe	a98a04d94464c62434e4fbc96b1de8a5d2d60ff1	infected
None	Files	C:\programdata\windowstask\xmrig-cuda.dll	ca16bbfc8960c138eb6dd6dfbae7ab1699642edb	infected
None	Files	C:\ProgramData\RealtekHD\taskhost.exe	46630105bb24f172e486eb7074feff92dd22493b	infected

Рисунок 23. 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.

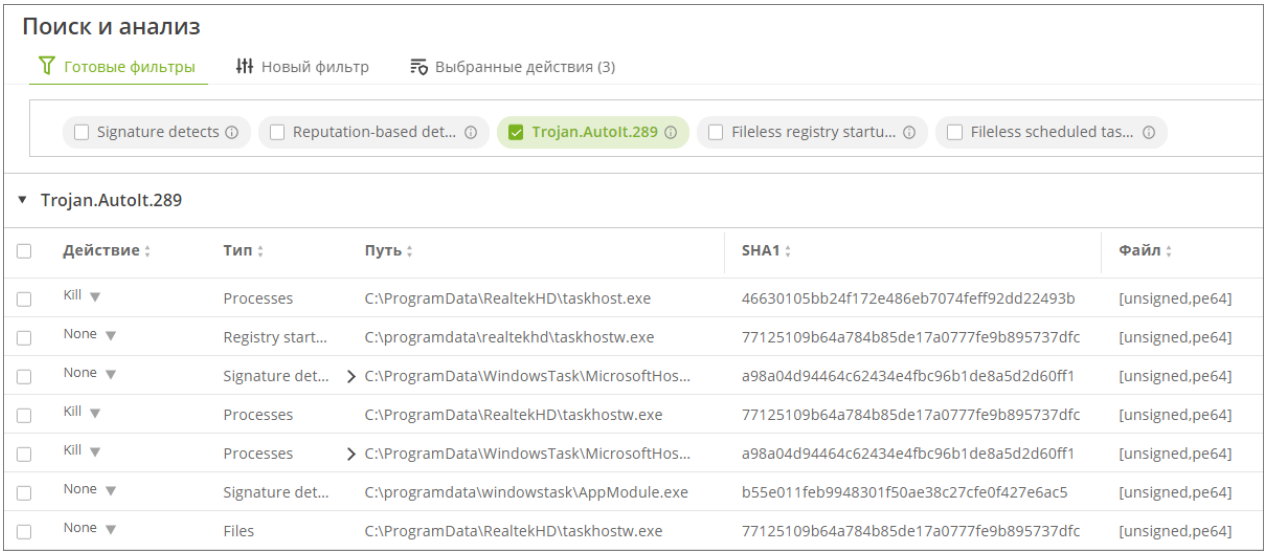

Рисунок 24. Фильтр Trojan.AutoIt.289

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**.

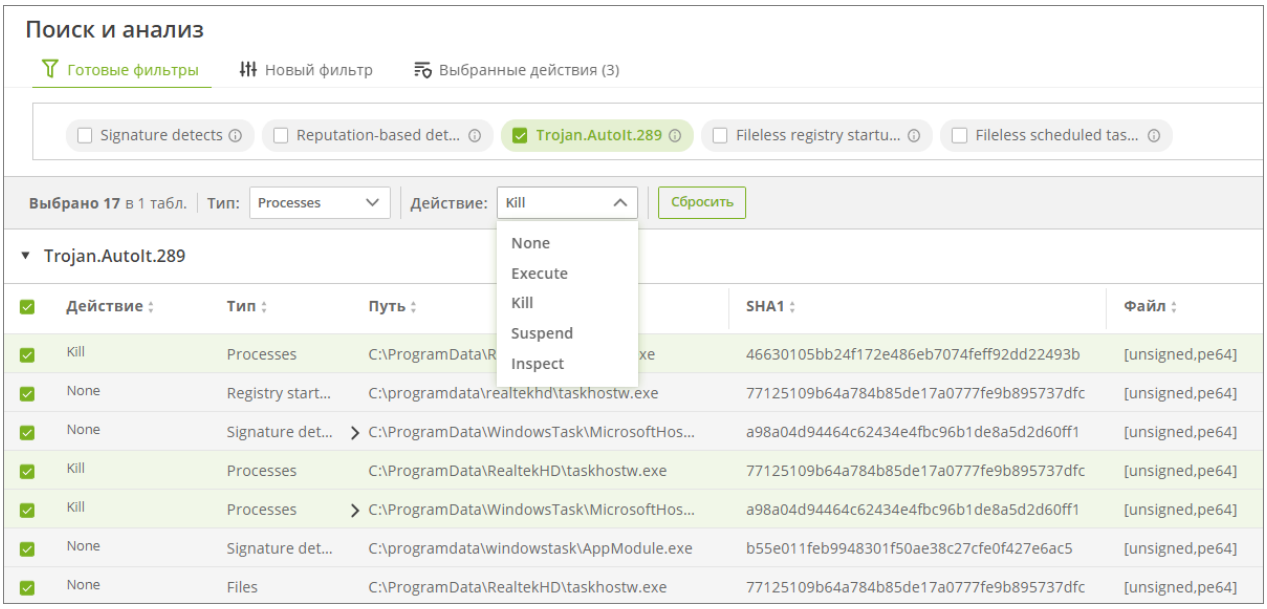

Рисунок 25. Выбор действий

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.

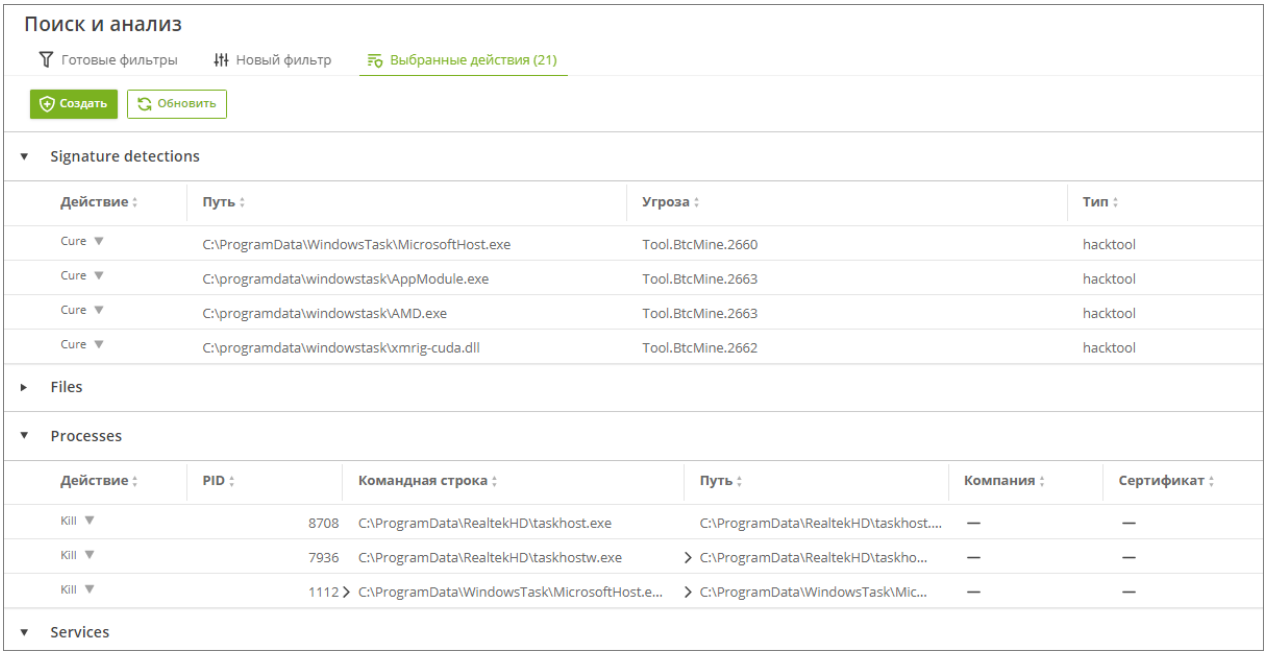

Рисунок 26. Выбранные действия

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.

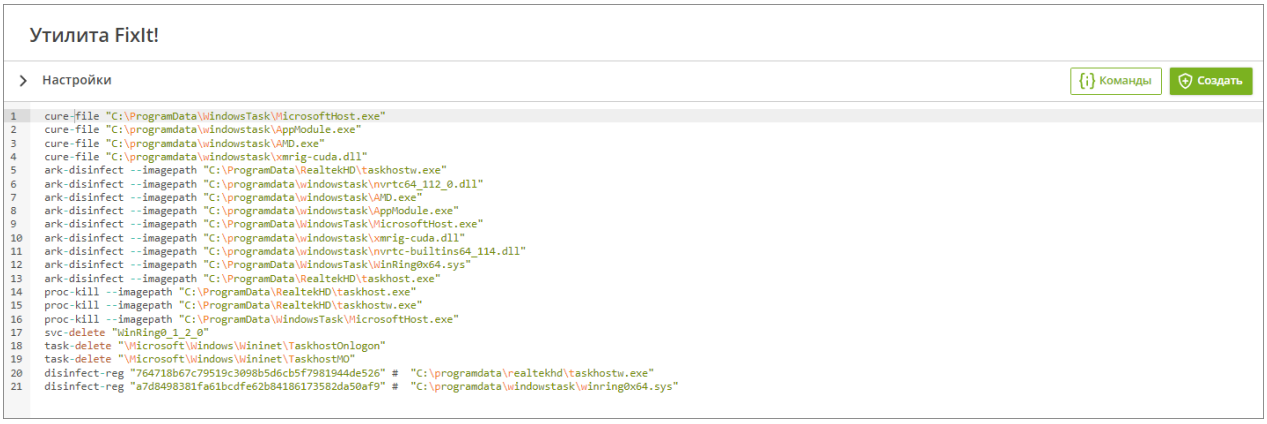

Рисунок 27. Готовый скрипт

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 выглядел так:

Рисунок 28. Скрипт после оптимизации

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

Итог

Проанализировав отчет, сформированный после лечения, с помощью функции Сравнение отчетов, мы убедились, что угроза была устранена.