

# Действия системного администратора в случае ВКИ на рабочей станции



## Действия системного администратора в случае ВКИ на рабочей станции

Dr.Web Enterprise Security Suite (далее – ES) обладает широкими возможностями по противодействию всем современным видам вредоносного ПО в автоматическом режиме без непосредственного участия пользователя и системного администратора.

Тем не менее, для своевременного аудита сети рекомендуем настроить автоматическую отправку оповещений в Центре управления ES-сервера. Для этого перейдите в раздел **Администрирование** и в блоке Оповещения выберите пункт **Конфигурация оповещений**.

Выберите **Метод отправки оповещений**, настройте Параметры и тип оповещений.

Оповещения об инцидентах могут:

- отображаться в веб-консоли Центра управления ES-сервера. Просмотреть их можно в блоке **Оповещения**, выбрав пункт **Оповещения веб-консоли**.

Администрирование > Оповещения веб-консоли

<input type="checkbox"/>	<input type="checkbox"/>	Время	Серьезность	Источник	Тема
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:17:33	Максимальная	Агент WIN-G3CDC09I0L4	Внимание! Об...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:17:08	Максимальная	Агент WIN-G3CDC09I0L4	Внимание! Об...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:14:38	Максимальная	Агент WIN-G3CDC09I0L4	Внимание! Обна...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:13:53	Максимальная	Агент WIN-G3CDC09I0L4	Внимание! Об...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:13:53	Максимальная	Агент WIN-G3CDC09I0L4	Внимание! Об...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:13:53	Максимальная	Агент WIN-G3CDC09I0L4	Внимание! Об...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:01:46	Минимальная	Агент WIN-G3CDC09I0L4	Установка на ...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:01:23	Минимальная	Сервер	Актуальное с...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:01:23	Минимальная	Сервер	Актуальное с...
<input type="checkbox"/>	<input type="checkbox"/>	19-10-2018 15:01:23	Минимальная	Сервер	Актуальное с...

1 2 3 4 Следующая —      Страница: 1      Показаны результаты 1 – 10 из 40

- передаваться по протоколу **SNMP** (Simple Network Management Protocol) для взаимодействия с внешними системами мониторинга.
- отправляться по электронной почте ответственным сотрудникам.

Администрирование > Конфигурация оповещений

- Администрирование
  - Сервер Dr.Web
  - Менеджер лицензий
  - Ключи шифрования
- Журналы
  - Журнал аудита
  - Журнал выполнения заданий
  - Журнал Сервера Dr.Web
  - Журнал обновлений репозитория
- Конфигурация
  - Администраторы
  - Аутентификация
  - Конфигурация Сервера Dr.Web
  - Удаленный доступ к Серверу Dr.Web
  - Планировщик заданий Сервера Dr.Web
  - Конфигурация веб-сервера
  - Пользовательские процедуры
- Оповещения
  - Оповещения веб-консоли
  - Неотправленные оповещения
  - Конфигурация оповещений
- Репозиторий
  - Состояние репозитория
  - Отложенные обновления
  - Общая конфигурация репозитория
  - Детальная конфигурация репозитория
    - Агент Dr.Web для Windows
    - Агент Dr.Web для UNIX
    - Агент Dr.Web для Android. Версия 10
    - Агент Dr.Web для Android. Версия 11
    - Сервер Dr.Web
    - Прокси-сервер Dr.Web
    - Виртуальные базы Dr.Web
    - Базы Spider Gate
    - Базы Антиспама Dr.Web
    - Новости компании "Доктор Веб"
    - Содержимое репозитория
- Дополнительные возможности

default

Метод отправки оповещений  
Электронная почта

[Редактировать общие заголовки](#)

Количество повторных отправок  
10

Тайм-аут повторной отправки  
300

Электронная почта получателей  
[ - ] [ + ]

[Отправить тестовое сообщение](#)

**Администраторы**

- Известный администратор
- Ошибка авторизации администратора

**Другое**

- Ошибка записи журнала Сервера
- Ошибка ротации журнала Сервера
- Соседний Сервер давно не подключался
- Статистический отчет
- Тестовое сообщение
- Эпизодия в сети

**Лицензия**

- Достигнуто ограничение по передаче лицензий
- Достигнуто ограничение по станциям в сети
- Истек срок передачи лицензий
- Окончание срока действия лицензионного ключа
- Превышено ограничение по станциям в группе
- Приближается ограничение по станциям в группе

**Новички**

- Станция ожидает подтверждения
- Станция отключена автоматически
- Станция отключена администратором

**Репозиторий**

- Актуальное состояние продукта в репозитории
- Запущено обновление продукта в репозитории
- Недостаточно свободного места на диске
- Обновление продукта в репозитории заморожено

**Станция**

- Аварийный разрыв соединения
- Критическая ошибка обновления станции
- Неизвестная станция
- Обнаружена угроза безопасности
- Ошибка авторизации станции
- Ошибка сканирования
- Ошибка создания учетной записи станции
- Станция давно не подключалась к Серверу
- Станция подтверждена автоматически
- Станция подтверждена администратором
- Станция уже зарегистрирована
- Статистика сканирования
- Требуется перезагрузка станции

**Установки**

- Установка на станции не выполнена
- Установка на станции успешно завершена

При обнаружении угрозы на защищаемом объекте установленное на нем антивирусное ПО обезвредит угрозу автоматически без участия пользователя. Тот получит сообщение об обнаруженной угрозе в виде всплывающего окна.

**Обнаружена угроза**  
Обнаружено и обезврежено угроз: **1**

[Подробнее](#)

При необходимости пользователь может посмотреть подробности, кликнув по ссылке [Подробнее](#).

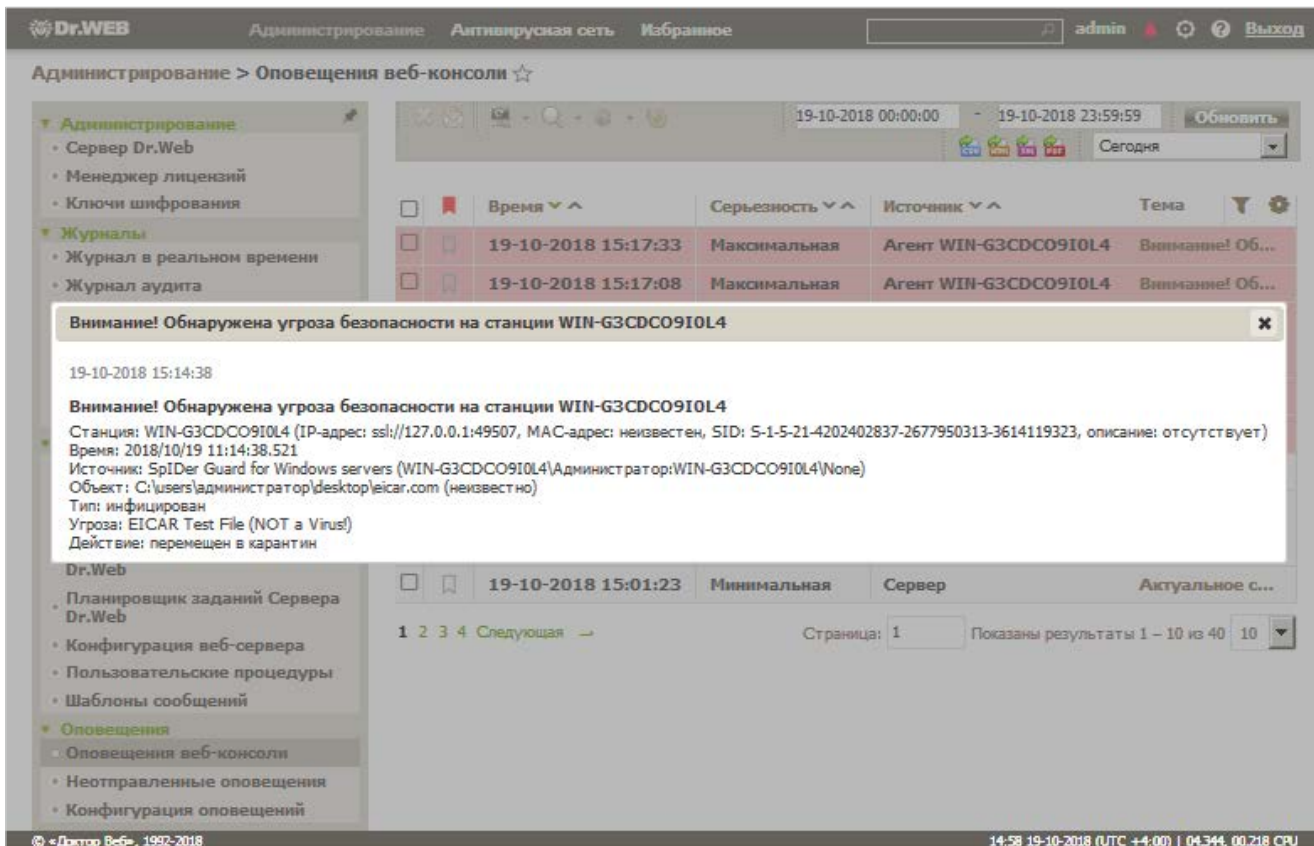
**Подробнее**

**Dr.Web обнаружил и обезвредил следующие вредоносные объекты**

Объект	Угроза	Действие	Путь
icar.com	EICAR Test File (...)	Перемещено	C:\users\администратор\appdata\local\te...

?

Запись об обнаруженной угрозе будет также передана в Центр управления ES-сервера в соответствии с заданными настройками оповещения.



The screenshot displays the Dr.Web administration console. The main window shows a list of alerts under the heading 'Оповещения веб-консоли'. A prominent notification window is open, displaying the following details:

- Внимание! Обнаружена угроза безопасности на станции WIN-G3CDCO9I0L4**
- 19-10-2018 15:14:38
- Внимание! Обнаружена угроза безопасности на станции WIN-G3CDCO9I0L4**
- Станция: WIN-G3CDCO9I0L4 (IP-адрес: ssl://127.0.0.1:49507, MAC-адрес: неизвестен, SID: 5-1-5-21-4202402837-2677950313-3614119323, описание: отсутствует)
- Время: 2018/10/19 11:14:38.521
- Источник: SpIDer Guard for Windows servers (WIN-G3CDCO9I0L4)Администратор:WIN-G3CDCO9I0L4(None)
- Объект: C:\users\администратор\desktop\eicar.com (неизвестно)
- Тип: инфицирован
- Угроза: EICAR Test File (NOT a Virus!)
- Действие: перемещен в карантин

The interface also shows a table of alerts with columns for 'Время', 'Серьезность', 'Источник', and 'Тема'. The status bar at the bottom indicates the system time as 14:58 on 19-10-2018 and CPU usage at 00.218.

### При получении оповещения об угрозе безопасности рекомендуем:

1. Открыть сообщение и ознакомиться с его деталями. Здесь содержится информация о наименовании защищаемого объекта (станции), где произошел инцидент, о компоненте антивирусного ПО, которое детектировало угрозу (источник), о зараженном объекте (объект), о наименовании угрозы (угроза) и произведенном с ним действии (действие).
2. Ознакомиться с описанием угрозы, найдя её по названию в вирусной базе Dr.Web: <https://vms.drweb.ru/search/>
3. Запланировать полное сканирование защищаемого объекта в нерабочее время. Для этого найдите в Антивирусной сети станцию, на которой произошел инцидент, и кликните по ней. В левом меню зайдите в раздел **Конфигурация** и выберите пункт **Планировщик задания**. Создайте задание, кликнув по иконке **Создать задание**. В открывшемся окне настройте параметры задания (действие: Сканер Dr.Web. Полное сканирование) и удобное время для его исполнения.



Антивирусная сеть > 1110d5a7-031b-4515-b151-1bf242374d41 | RAIDEN-ПК | tcp://194.85.20.253:61999 > Планировщик заданий > Создать задание

Выбранные объекты

- Общие
  - Графики
  - Идентификаторы безопасности
  - Запущенные компоненты
  - Установленные компоненты
  - Оборудование и программы
  - Свойства
- Статистика
  - Угрозы
  - Сводные данные
  - Ошибки
  - Статистика сканирования
  - Запуск/Завершение
  - Статистика угроз
  - Состояние
  - Продукты
  - Вирусные базы
  - Модули
  - Инсталляции Агентов
  - Деинсталляции Агентов
- Конфигурация
  - Права
  - Планировщик заданий
  - Устанавливаемые компоненты
  - Ограничения обновлений
  - Параметры подключения
  - Сканер
  - SPIDER Guard для рабочих станций
  - SPIDER Mail
  - SPIDER Gate
  - Родительский контроль
  - Агент Dr.Web
  - Превентивная защита
  - Dr.Web для Microsoft Outlook

Создать задание

Общие Действие Время

Действие: Сканер Dr.Web. Полное сканирование

Действия	Ограничения
Инфицированные	Лечить
Подозрительные	Перемещать в карантин
Неизлеченные	Перемещать в карантин
Инфицированные установочные пакеты	Перемещать в карантин
Инфицированные архивы	Перемещать в карантин
Инфицированные почтовые файлы	Перемещать в карантин
Инфицированные загруженные секторы	Лечить
Рекламные программы	Перемещать в карантин
Программы-ловушки	Перемещать в карантин
Программы-шутки	Перемещать в карантин
Потенциально опасные	Перемещать в карантин
Программы-вызовы	Перемещать в карантин

Приоритет сканирования:

Уровень загрузки ресурсов компьютера:

Действия после сканирования

Получите от пользователей ПК, на котором произошел инцидент, перечень внешних запоминающих устройств (флэшек, дисков и т. п.), которые к нему подключались, и выполните их проверку антивирусным сканером. Также необходимо проверить все компьютеры, к которым эти устройства подключались ранее.

**Внимание!!!** В случае заражения устройства троянцем-шифровальщиком (энкодером), незамедлительно отключите компьютер и обратитесь в службу технической поддержки [https://support.drweb.ru/new/free\\_unlocker/for\\_decode](https://support.drweb.ru/new/free_unlocker/for_decode).

При этом запрещается производить сканирование диска антивирусным сканером любого производителя, поскольку из-за этого расшифровка диска будет невозможна.

4. Если загрузка операционной системы на защищаемом объекте не производится после повреждения системных файлов вирусом, измените настройки BIOS компьютера, чтобы обеспечить возможность загрузки ПК с компакт-диска или USB-накопителя.

Скачайте образ аварийного диска восстановления системы Dr.Web LiveDisk или утилиту записи Dr.Web LiveDisk на USB-накопитель, подготовьте соответствующий носитель. Загрузив компьютер с использованием этого носителя, выполните полную проверку и лечение обнаруженных угроз.

Адрес для скачивания: [https://free.drweb.ru/aid\\_admin/](https://free.drweb.ru/aid_admin/).

**Внимание!** Обязательно знакомьтесь с документацией перед использованием!

5. В случае возникновения инцидента на мобильном устройстве необходимо загрузить смартфон или планшет в безопасном режиме (в зависимости от версии операционной системы и особенностей конкретного устройства эта процедура может быть выполнена различными способами; обратитесь за уточнением к инструкции, поставляемой вместе с приобретенным аппаратом, или напрямую к его производителю) и произвести полную проверку системы, выполнив рекомендации по нейтрализации обнаруженных угроз. Затем выключите устройство и включите его в обычном режиме.
6. В случае наличия подозрения на ложное срабатывание антивирусного ПО на защищаемом объекте или при пропуске вредоносных ссылок в Офисном контроле сообщите об этом по адресу: <https://support.drweb.ru/new/urlfilter/>.

В случае необходимости проверки подозрительного объекта, почтового вложения или ссылки в интернете, на которые не производится срабатывание антивирусного ПО, отправьте их в вирусную лабораторию Dr.Web для проверки: <https://vms.drweb.ru/sendvirus/>

По любым вопросам, связанным с вирусными инцидентами, обращайтесь в техническую поддержку Dr.Web: <https://support.drweb.ru>

## О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании. Вот только некоторые клиенты Dr.Web: <https://customers.drweb.com>.

**Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

## Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недеklarированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
- Использование ПО Dr.Web позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:
  - информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
  - отдельных категорий граждан от информации, причиняющей вред.

<a href="#"><u>Сертификаты ФСТЭК России</u></a>	<a href="#"><u>Сертификаты Минобороны России</u></a>	<a href="#"><u>Сертификаты ФСБ России</u></a>	<a href="#"><u>Все сертификаты и товарные знаки</u></a>
---	--	---	---

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.



© ООО «Доктор Веб»,  
2003–2018

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а  
Тел.: +7 495 789–45–87 (многоканальный)  
Факс: +7 495 789–45–97

<https://антивирус.рф> | <https://www.drweb.ru> | <https://curenet.drweb.ru> | <https://free.drweb.ru>