

Контент-фильтр

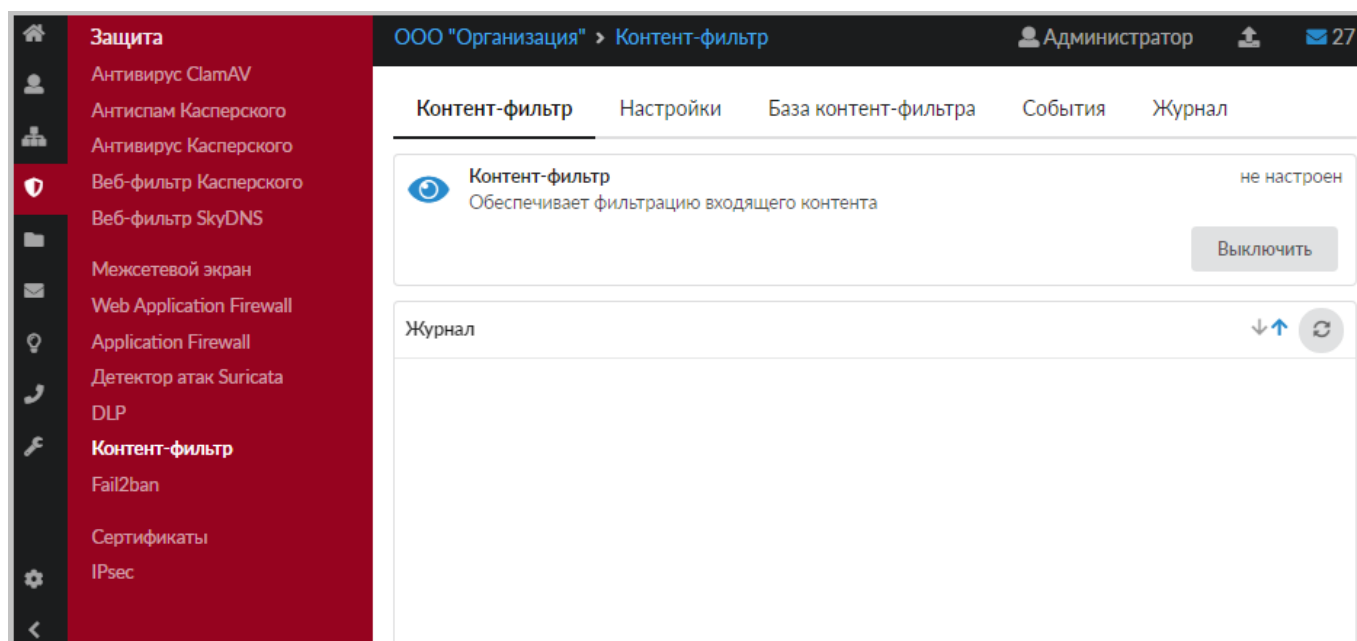
Модуль «Контент-фильтр» расположен в Меню «Защита». Модуль предназначен для настройки и блокировки интернет-страниц, содержащих в себе заданные ключевые слова или регулярные выражения. Модуль «Контент-фильтр» имеет вкладки:

- «Контент-фильтр»;
- «Настройки»;
- «База Контент-фильтра»;
- «События»;
- «Журнал».

Для применения контентной фильтрации трафика, необходимо в Меню - «Наборы правил» добавить в один/несколько наборов [«Правило контентной фильтрации»](#). В данном случае, правило/правила примененные к Пользователю/группе Пользователей будут использовать контентную фильтрацию трафика. Или в индивидуальном модуле Пользователя/Группы Пользователей на вкладке [«Правила и ограничения»](#) добавить «Правило контентной фильтрации». Стоит отметить, что для корректного функционирования контентной фильтрации необходимо [расшифровывать трафик](#) полностью.

Контент-фильтр

Вкладка «Контент-фильтр». Отображает состояние модуля контент-фильтра запущен/остановлен/не настроен, также отображает журнал модуля за текущую дату, имеет кнопку включения/выключения.



После регистрации «ИКС» (Меню «Обслуживание» - [«О программе»](#)) и настройки Контент-фильтра, окно «Контент-фильтр» будет выглядеть так:

Скриншот интерфейса модуля «Контент-фильтр» в разделе «Защита». Вверху панели навигации отображены: «Защита», «Антивирус ClamAV», «Антиспам Касперского», «Антивирус Касперского», «Веб-фильтр Касперского», «Веб-фильтр SkyDNS», «Межсетевой экран», «Web Application Firewall», «Application Firewall», «Детектор атак Suricata», «DLP», «Контент-фильтр» (выделено), «Fail2ban», «Сертификаты», «IPsec». В заголовке страницы: «ООО "Организация" > Контент-фильтр», «Администратор», «10». Вкладки: «Контент-фильтр», «Настройки», «База контент-фильтра», «События», «Журнал». Основной блок «Контент-фильтр» содержит иконку глаза, название «Контент-фильтр», описание «Обеспечивает фильтрацию входящего контента» и статус «запущен». Кнопка «Выключить». Ниже — таблица «Журнал» с записями:

Журнал
Download finished 16:05:17
Update done. Current version base 9.00 16:05:17
started 16:05:19
ebus client [cf] connected 16:05:19
exited 16:05:20
started 16:05:20
ebus client [cf] connected 16:05:20

Состояние работы модуля изменится на «запущен», в журнале появятся записи логов.

Настройки

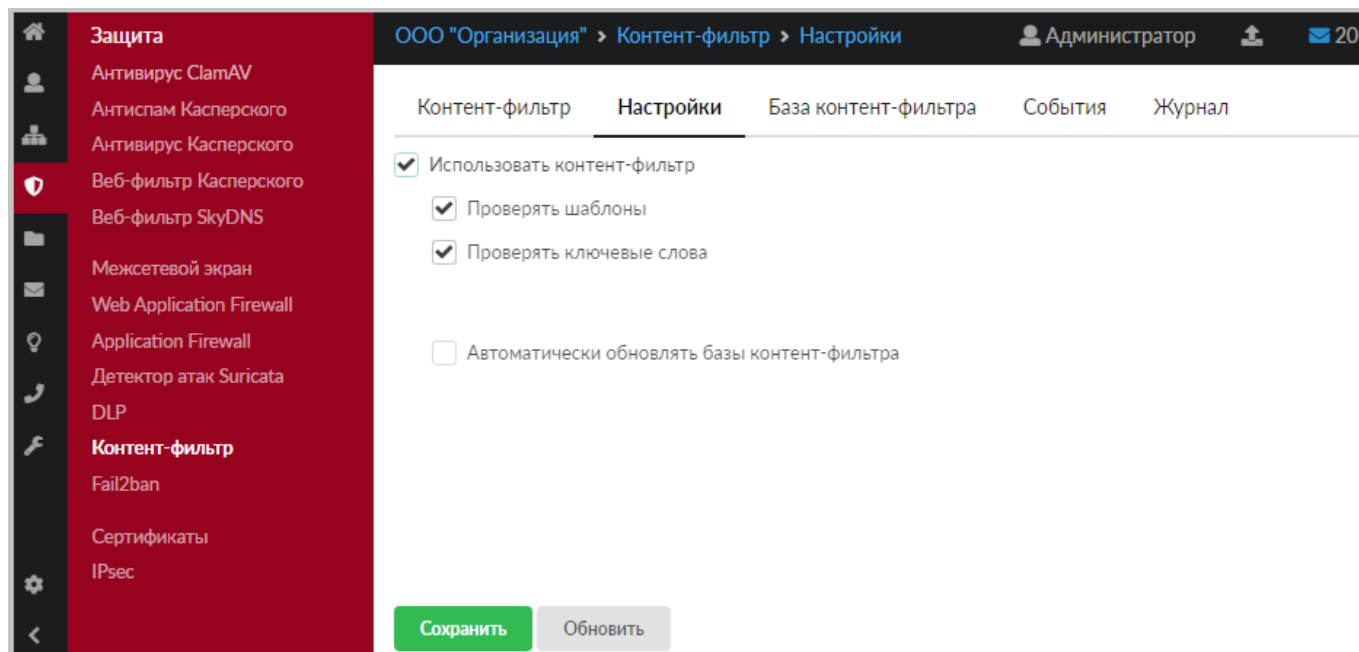
Вкладка «Настройки» содержит флаги управления состоянием модуля, обновлением его баз и вариантами фильтрации. Сразу после установки «ИКС» флаги вкладки «Настройки» не выставлены:

Скриншот интерфейса модуля «Контент-фильтр» в разделе «Защита». Вкладки: «Контент-фильтр», «Настройки» (выделено), «База контент-фильтра», «События», «Журнал». Основные настройки:

- ☐ Использовать контент-фильтр
 - ☐ Проверять шаблоны
 - ☐ Проверять ключевые слова
- ☐ Автоматически обновлять базы контент-фильтра

Кнопки: «Сохранить», «Обновить».

Включение флага «Использовать контент-фильтр» автоматически включает флаги «Проверять шаблоны» и «Проверять ключевые слова». Флаг «Автоматически обновлять контент-фильтр» выставляется отдельно при необходимости.



Важно. После установки «ИКС» списки баз модуля «Контент-фильтр» - пустые. Если флаг «Автоматически обновлять контент-фильтр» не включен, то для фильтрации необходимо создать и заполнить списки баз вручную.

Рекомендуется устанавливать флаг «Автоматически обновлять контент-фильтр» для использования уже готовых баз. Модуль подключится к облачному сервису и загрузит последнюю версию списков. В дальнейшем, при установленном флажке, списки будут обновляться раз в сутки.

Важно. Чтобы настройки вступили в силу необходимо нажать кнопку «Сохранить». Далее необходимо проверить, что базы обновились - на вкладке «База Контент-фильтра». Нужно выбрать один из списков слов. Если обновление прошло удачно, то под названием выбранного списка появится несколько ключевых слов и шаблонных выражений из этого списка.

База Контент-фильтра

Вкладка «База Контент-фильтра» позволяет:

- управлять базами «Контент-фильтра»;
- редактировать списки шаблонов и слов баз;
- включать/выключать отдельную базу в работу модуля;
- удалять базы;
- искать шаблоны и слова в базах.

Важно. По-умолчанию, модуль «Контент-фильтр» содержит ПУСТЫЕ списки слов, запрещенных Минюстом и Госнаркоконтролем, а также специальный список облачного сервиса SkyDNS. Они не содержат записей. Для получения данных записей необходимо иметь лицензию на обновление.

Каждая база содержит две вкладки - шаблоны и ключевые слова. Их просмотр и редактирование доступно в диалоговом окне «Редактирование группы слов контент-фильтра» при нажатии кнопки «Редактировать» в окне вкладки или в блоке базы при её выделении.

Вкладка «Ключевые слова» - позволяет задать любой длины строку, содержащую любые символы. Контент-фильтр сработает на данную строку, если перед и после указанной строки идет любой символ, кроме буквенного. Например, задано - «ет Са», контент-фильтр не сработает на «Привет Саша», но сработает на «Прив-ет Са».

Вкладка «Шаблоны» - позволяет задать регулярные выражения. Например:

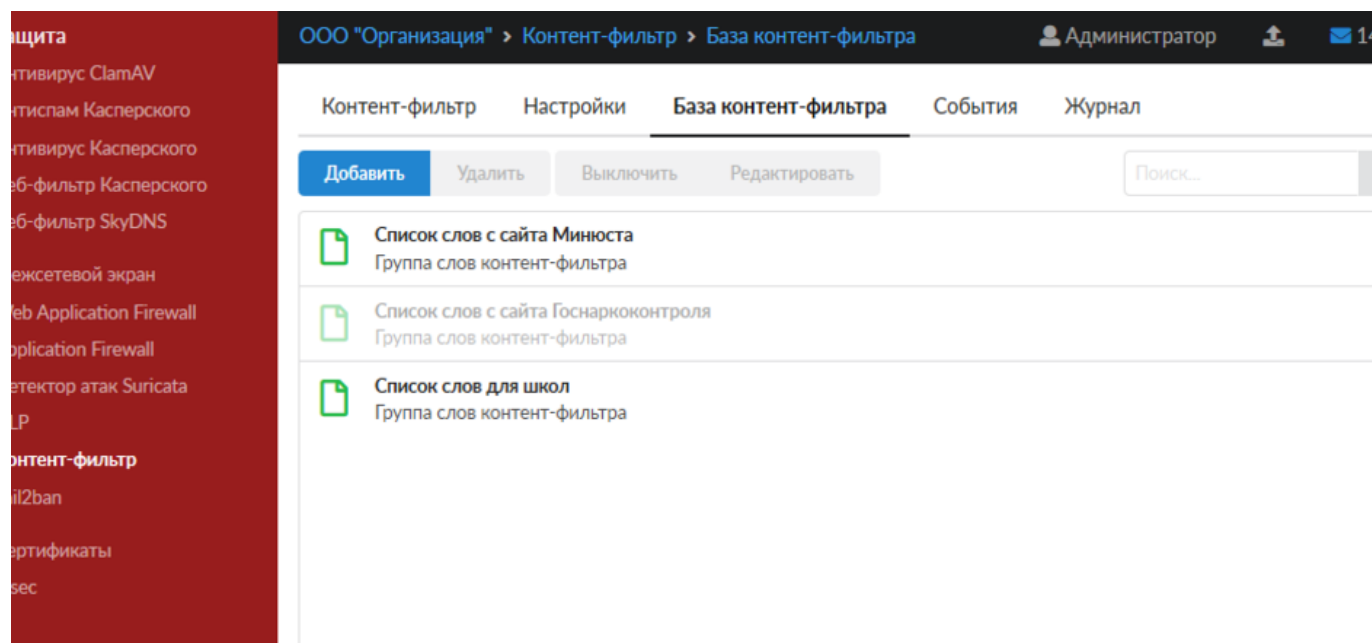
- **Привет** - Контент-фильтр будет искать не изменяемое регулярное выражение - «Привет»
- **/\bрус.*\b/** - Контент-фильтр сработает на слова: русич, русский, русофоб, рус.яз

При добавлении регулярного выражения в шаблоны, необходимы придерживаться конструкции - **/регулярное выражение/**. Само регулярное выражение задается по

общепринятым нормам. Кратко почитать о регулярных выражениях возможно тут <https://tproger.ru/articles/regexp-for-beginners/>. Стоит отметить, что буква «ё» воспринимается как буква «е».

Важно. Модуль «Контент-фильтр» производит фильтрацию контента по списку шаблонов и списку ключевых слов, которые состоят из общих списков соответствующих шаблонов и слов каждой из включенных баз. Фильтрация по шаблонам и словам выключенной базы производится не будет.

Выключенная база в окне вкладки «База Контент-фильтра» выглядит неактивной - затенена.



Редактирование группы слов контент-фильтра

Диалоговое окно «Редактирование группы слов контент-фильтра» позволяет добавлять и удалять шаблоны и ключевые слова.

Редактирование группы слов контент-фильтра

Шаблоны

Ключевые слова

Добавить

Удалить

Импорт

Экспорт

2890 записей

1488

21sextury

50921688334548

7pgb1h44vg08

abrek

abshabashennyi

abstiag

abstiaga

abstiak

adiveda

adult

Сохранить

Отмена

Для экспорта списка «Шаблоны» или «Ключевые слова» необходимо выбрать соответствующую вкладку и нажать кнопку «Экспорт». Список будет загружен браузером с именем файла - <Имя базы>-<тип списка>.txt, например - «Список слов с сайта Госнаркоконтроля-regex.txt».

Добавить свой список шаблонов или ключевых слов можно по кнопке «Импорт». Файл должен содержать список шаблонов или слов (каждое с новой строки) в формате *.txt.

Поиск шаблонов и слов в базах

Поиск шаблонов и ключевых слов в списках баз модуля «Контент-фильтр» происходит с использованием поискового поля. При наборе слов шаблона происходит динамический поиск по базам, в результате в окне вкладки «База Контент-фильтра» в списке баз остаются только базы, содержащие искомое выражение.

Защита

Антивирус ClamAV

Антиспам Касперского

Антивирус Касперского

Веб-фильтр Касперского

Веб-фильтр SkyDNS

Межсетевой экран

Web Application Firewall

Application Firewall

Детектор атак Suricata

DLP

Контент-фильтр

Fail2ban

Сертификаты

sec

ООО "Организация" > Контент-фильтр > База контент-фильтра

Администратор

Контент-фильтр

Настройки

База контент-фильтра

События

Журнал

Добавить

Удалить

Выключить

Редактировать

1488

Список слов с сайта Минюста

Группа слов контент-фильтра

1488, 1488 скинхэд патриот россии, 1488 – скинхэд – патриот россии, 2018 жа?ар ай кудайды? бергенин бичип алган кижии ленчинова, 2018, жа?ар ай кудайды? бергенин бичип алган кижии ленчинова, ...

Удалить

Редактировать

Выключить

Список слов для школ

Группа слов контент-фильтра

Защита

Антивирус ClamAV

Антивирус DrWeb

Антиспам Касперского

Антивирус Касперского

Веб-фильтр Касперского

Межсетевой экран

Web Application Firewall

Детектор атак Suricata

DLP

Контент-фильтр

Fail2ban

Сертификаты

ООО "Организация" > Контент-фильтр > База Контент-фильтра

Администратор

Контент-фильтр

Настройки

База Контент-фильтра

События

Журнал

Добавить

Удалить

Выключить

Редактировать

1488

Список слов с сайта Минюста

Группа слов контент-фильтра

1488, 2018 жаңар ай кудайдын бергенин бичип алган кижии ленчинова, 2018, жаңар ай кудайдын бергенин бичип алган кижии ленчинова

Редактировать

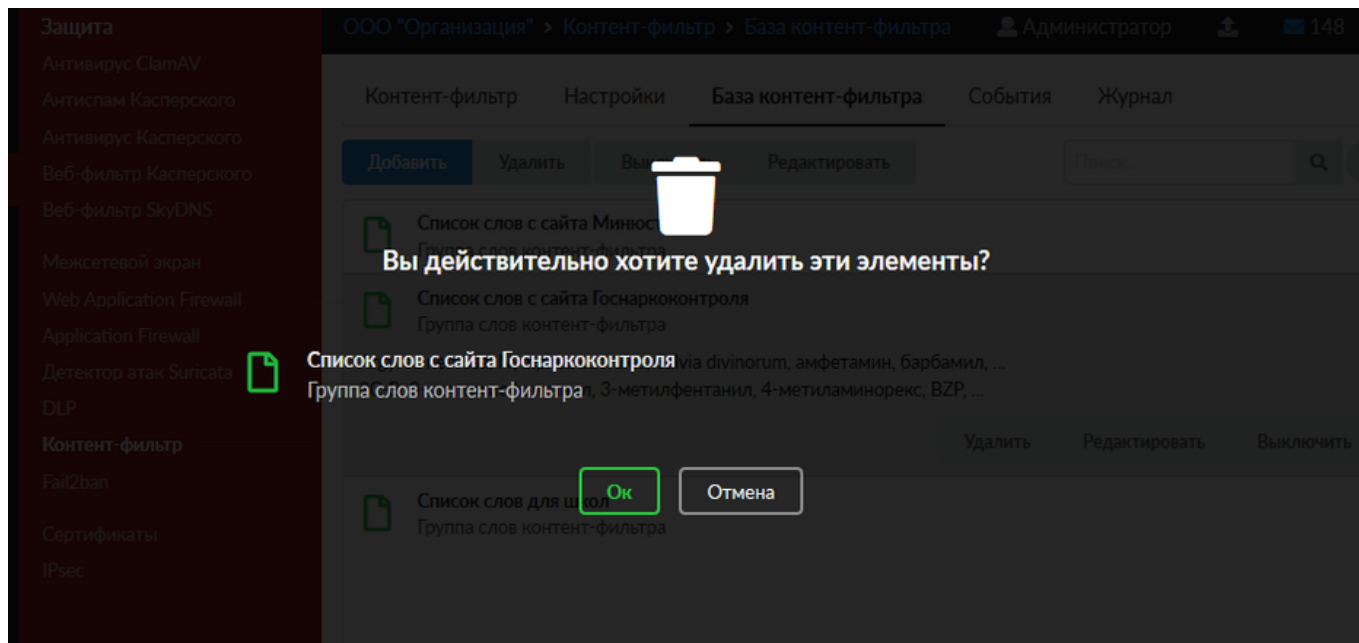
Выключить

Список слов для школ, по данным сервиса SkyDNS

Группа слов контент-фильтра

Удаление списка из Базы контент-фильтра

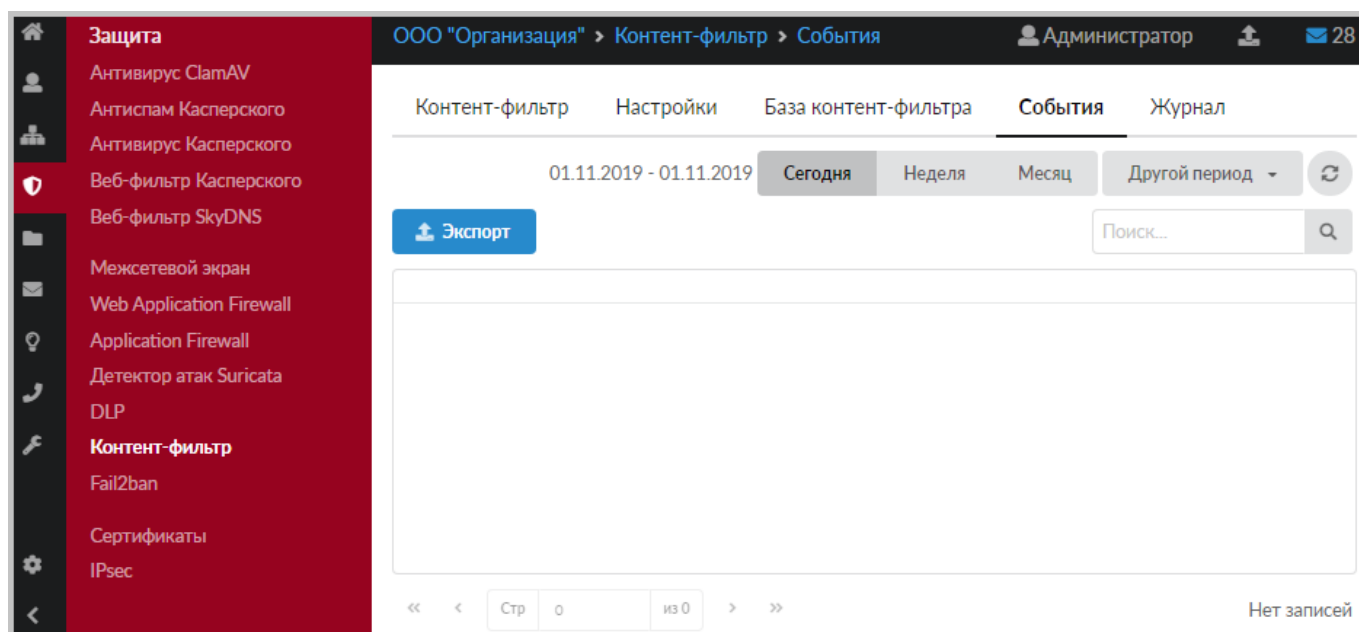
Удаление неиспользуемого списка из базы контент-фильтра происходит по кнопке «Удалить» при его выделении:



Важно. При удалении списков Базы по-умолчанию (Минюст, Госнаркоконтроль и SkyDNS), вернуть их обратно НЕЛЬЗЯ. Прежде чем их удалять воспользуйтесь механизмом экспорта списков.

События

Вкладка «События» позволяет просматривать, фильтровать и экспортировать информацию о блокировках контента. Возможен отбор событий за текущий день, неделю, месяц. Для точного поиска можно задать период вручную.



При работе Пользователей «ИКС» с сайтами Интернет, модуль «Контент-фильтр» будет производить проверку контента. Все заблокированные ресурсы будут отображаться в окне вкладки «События» с пояснением по шаблону или слову произошла блокировка.

ООО "Организация" > Контент-фильтр > События

Администратор 35

Контент-фильтр Настройки База контент-фильтра **События** Журнал

01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период ↻

Экспорт Поиск...

Запрещён доступ на s7.addthis.com с адреса 192.168.17.4 по ключевому слову "xxx"	14:21:57
Запрещён доступ на appttractor.ru с адреса 192.168.17.4 по ключевому слову "bang"	14:21:52
Запрещён доступ на edu.devto.dev.com с адреса 192.168.17.4 по ключевому слову "strip"	14:21:49
Запрещён доступ на tproger.ru с адреса 192.168.17.4 по ключевому слову "хардкор"	14:21:44
Запрещён доступ на habr.com с адреса 192.168.17.4 по ключевому слову "мда"	14:21:44
Запрещён доступ на cryptoworld.su с адреса 192.168.17.4 по ключевому слову "bang"	14:21:44

« < Стр 1 из 1 > » Показаны записи 1 - 13 из 13

Посмотреть **полный URL заблокированного ресурса** можно щёлкнув по строке с событием:

ООО "Организация" > Контент-фильтр > События

Администратор 35

Контент-фильтр Настройки База контент-фильтра **События** Журнал

01.11.2019 - 01.11.2019 Сегодня Неделя Месяц Другой период ↻

Экспорт Поиск...

Запрещён доступ на s7.addthis.com с адреса 192.168.17.4 по ключевому слову "xxx"	14:21:57
Запрещён доступ на appttractor.ru с адреса 192.168.17.4 по ключевому слову "bang"	14:21:52
Запрещён доступ на edu.devto.dev.com с адреса 192.168.17.4 по ключевому слову "strip"	14:21:49
Запрещён доступ на tproger.ru с адреса 192.168.17.4 по ключевому слову "хардкор"	14:21:44
Запрещён доступ на habr.com с адреса 192.168.17.4 по ключевому слову "мда"	14:21:44
Запрещён доступ на cryptoworld.su с адреса 192.168.17.4 по ключевому слову "bang"	14:21:44

« < Стр 1 из 1 > » Показаны записи 1 - 13 из 13

Для поиска по событиям есть поисковое поле.

Важно. Кнопка «Удалить логи» удаляет все логи, которые ведутся модулем «Контент-фильтр».

Журнал

Вкладка «Журнал» отображает сводку всех системных сообщений модуля «Контент-фильтр» с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад»

возможно переходить со страницы на страницу, либо ввести номер требуемой страницы.

The screenshot displays the 'Журнал' (Log) section of the 'Контент-фильтр' (Content Filter) module. The sidebar on the left lists various security modules under the 'Защита' (Protection) heading, with 'Контент-фильтр' (Content Filter) currently selected. The top navigation bar shows the breadcrumb 'ООО "Организация" > Контент-фильтр > Журнал' and the user 'Администратор'. The main area has tabs for 'Контент-фильтр', 'Настройки', 'База контент-фильтра', 'События', and 'Журнал'. The 'Журнал' tab is active, showing a date range of '01.11.2019 - 01.11.2019' and buttons for 'Сегодня', 'Неделя', 'Месяц', and 'Другой период'. There are also buttons for 'Экспорт' (Export) and 'Удалить логи' (Delete logs), and a search bar labeled 'Поиск...'. The log entries are listed in a table with columns for the event name and time. The entries include 'Download finished', 'Update done. Current version base 9.00', 'started', 'ebus client [cf] connected', and 'exited'. The bottom of the log area shows pagination: 'Стр. 1 из 1' and 'Показаны записи 1 - 7 из 7'.

В правом верхнем углу модуля находится строка поиска, а также возможность выбора периода отображения журнала событий. По-умолчанию, журнал отображает события за текущую дату. При необходимости можно сохранить данные журнала в файл, нажав кнопку «Экспорт» или удалить данные журнала, за определенный период, нажав кнопку «Удалить логи».

Важно. Кнопка «Удалить логи» удаляет ВСЕ логи, которые ведутся модулем «Контент-фильтр».

From:

<https://doc-old.a-real.ru/> - **Документация**

Permanent link:

<https://doc-old.a-real.ru/doku.php?id=ics70:content&rev=1573397037>

Last update: **2020/01/27 16:28**

