# 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 - Пользователи и статистика - Наборы правил добавить в один или 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.

*	Защита	000 "(	Организация" >	Контент-фильт	р	🚨 Админист	ратор	£	<b>2</b> 7
٠	Антивирус ClamAV Антиспам Касперского	Конт	гент-фильтр	Настройки	База контент-фильтра	События	Журнал	1	
#	Антивирус Касперского		· ·						
Ð	Веб-фильтр Касперского	0	Контент-фильтр	) ИЛЬТЮЗНИЮ ВХОЛЯ				не наст	гроен
	Веб-фильтр SkyDNS		oocene waaer y	илы рацию входи	dero kontenta		c c		
	Межсетевой экран							וארטזולאומל	
	Web Application Firewall	Журна	ал					<b>↓</b> ↑	3
ç	Application Firewall								
ى									
۶	Контент-фильтр								
	Fail2ban								
	Сертификаты								
٠	IPsec								
<									

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

*	Защита	ООО "Организация" > Контент-фильтр	💄 Админист	ратор 🏦	<b>V</b> 10
≗ ≟	Антивирус ClamAV Антиспам Касперского Антивирус Касперского Веб-фильтр Касперского Веб-фильтр SkyDNS	Контент-фильтр Настройки База контент-фильтра Монтент-фильтр Обеспечивает фильтрацию входящего контента	События	Журнал	апущен
	Межсетевой экран			Выклю	чить
ç	Web Application Firewall Application Firewall	Журнал		4	↑ C
و	Детектор атак Suricata DI P	Download finished 16:05:17			
F	Контент-фильтр	Update done. Current version base 9.00 16:05:17			
	Fail2ban	started 16:05:19			
	Сертификаты IPsec	ebus client [cf] connected 16:05:19			
		exited 16:05:20			
		started 16:05:20			
* <		ebus client [cf] connected			

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:

*	Защита	ООО "Организация"	Контент-фил	ьтр <b>&gt;</b> Настройки	💄 Админис	гратор 🛃	<b>2</b> 0 🔁
<u>.</u>	Антивирус ClamAV						
_	Антиспам Касперского	Контент-фильтр	Настройки	База контент-фильтра	События	Журнал	
÷.	Антивирус Касперского						
Ð	Веб-фильтр Касперского		ент-фильтр				
_	Веб-фильтр SkyDNS	Проверять шаб	блоны				
	Межсетевой экран	Проверять клк	очевые слова				
	Web Application Firewall						
ç	Application Firewall	Автоматически	и обновлять базь	контент-фильтра			
,	Детектор атак Suricata			nomeni grintipu			
~	DLP						
×	Контент-фильтр						
	Fail2ban						
	Сертификаты						
٠	IPsec						
<		Сохранить Обн	ЮВИТЬ				

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

*	Защита	ООО "Организация"	Контент-филь	💄 Админис	тратор 🛃	<b>2</b> 0 🔁	
•	Антивирус ClamAV						
	Антиспам Касперского	Контент-фильтр	Настройки	База контент-фильтра	События	Журнал	
÷	Антивирус Касперского		тент-фильтр				
<b>v</b>	Веб-фильтр Касперского						
-	Веб-фильтр SkyDNS	Проверять ша	блоны				
	Межсетевой экран	🖌 Проверять кл	ючевые слова				
	Web Application Firewall						
Ŷ	Application Firewall	Автоматическ	и обновлять базы	контент-фильтра			
	Детектор атак Suricata			·····			
-	DLP						
F	Контент-фильтр						
	Fail2ban						
	Сертификаты						
٠	IPsec						
<		Сохранить Об	новить				

**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 выберать 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 для школ. Они не содержат записей. Для получения данных записей необходимо иметь активный *модуль «Техподдержка»* (в первый год действует по умолчанию у всех клиентов, далее требуется его ежегодное приобретение).



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.

*	Защита	ООО "Организация" > Контент-фильтр > База контент-фильтра	💄 Администратор 🏻 🔒	<b>2</b> 146 😯
<b>≗</b> .≞	Антивирус ClamAV Антиспам Касперского Антивирус Касперского	Контент-фильтр Настройки База контент-фильтра События	Журнал	
D	Веб-фильтр Касперского	Добавить Удалить Выключить Редактировать		Q 2
•	Веб-фильтр SkyDNS	Список слов с сайта Минюста Группа слов контент-фильтра		
	Межсетевои экран Web Application Firewall	Список слов с сайта Госнаркоконтроля		
ہ ر	Application Firewall Детектор атак Suricata DLP	Argyrea nervosa, Nymphea caerulea, Salvia divinorum, амфетамин, барбамил, 2C-B, 3-метилтиофентанил, 3-метилфентанил, 4-метиламинорекс, BZP,		
×	Контент-фильтр		Удалить Редактировать	Выключить
	Fail2ban Сертификаты IPsec	Список слов для школ Группа слов контент-фильтра		

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»
- /\bpyc.\*\b/ Контен-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.

*	Защита	ООО "Организация" > Контент-фильтр > База контент-фильтра	💄 Администратор 🛛 🟦	<b>147</b>
<b>≗</b> ♣	Антивирус ClamAV Антиспам Касперского Антивирус Касперского	Контент-фильтр Настройки <b>База контент-фильтра</b> События	Журнал	
Ð	Веб-фильтр Касперского	Добавить Удалить Выключить Редактировать		Q 2
	Веб-фильтр SkyDNS Межсетевой экран Web Application Firewall Application Firewall	Список слов с сайта Минюста Группа слов контент-фильтра     Список слов с сайта Госнаркоконтроля Группа слов контент-фильтра		
ر ۶	Детектор атак Suricata DLP Контент-фильтр Fail2ban Сертификаты IPsec	Список слов для школ Группа слов контент-фильтра		

#### 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	Ключевы	е слова							
Добавить	Удалить	🛓 Импорт	🛓 Экспорт		2890 sa	писей 2			
1488									
21sextury									
509216883345	548								
7pgb1h44vg08									
abrek									
abshabashenny	i								
abstiag									
abstiaga									
abstiak									
adiveda									
adult									
				Coxt	ранить	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-regexp.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.



#### 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.

*	Защита	ООО "Органи	зация"	• Контент-филы	💄 Администратор 🔒 👔				
•	Антивирус ClamAV								
	Антиспам Касперского	Контент-фи	ільтр	Настройки	База контен	нт-фильтра	Событи	<b>ія</b> Журнал	
æ	Антивирус Касперского		04.44	0040 0444 0040	6				~
<b>O</b>	Веб-фильтр Касперского		01.11	.2019 - 01.11.2019	Сегодня	Неделя	Месяц	Другои период 👻	9
	Веб-фильтр SkyDNS	🛓 Экспорт						Поиск	Q
_	Межсетевой экран								
	Web Application Firewall								
Ŷ	Application Firewall								
,	Детектор атак Suricata								
۳	DLP								
۶	Контент-фильтр								
	Fail2ban								
	Сертификаты								
۵	IPsec								
<		«« « Стр	0	из 0 🔹	>>			He	г записей

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.

*	Защита	ООО "Организаци	ия" > Контент-фил	ьтр > Событи	я	🚨 Адми	нистратор 🟦	<b>S</b> 35			
٩	Антивирус ClamAV Антиспам Касперского	Контент-фильт	р Настройки	База контен	нт-фильтра	События	я Журнал				
<b>#</b>	Антивирус Касперского										
Ð	Веб-фильтр Касперского	0	1.11.2019 - 01.11.201	.9 Сегодня	Неделя	Месяц	Другой период	- <i>C</i>			
•	Веб-фильтр SkyDNS	🛓 Экспорт					Поиск	Q			
_	Межсетевой экран										
	Web Application Firewall	2200 North 10 s7 addthis com s appear 192 149 17 4 no valevenov v sporv "vvv"									
ç	Application Firewall	14:21:57	Запрещен доступ на s7.addtnis.com с адреса 192.108.17.4 по ключевому слову XXX 14:21:57								
,	Детектор атак Suricata	Запрещён доступ 14:21:52	на apptractor.ru с адр	eca 192.168.17.4	4 по ключевом	ıy слову "ban	g"				
۶	Контент-фильтр	Запрещён доступ 14:21:49	на edu.devtodev.com	с адреса 192.16	8.17.4 по ключ	евому слову	' "strip"				
	Fail2ban	Запрещён доступ 14:21:44	на tproger.ru с адреса	192.168.17.4 no	о ключевому с	лову "хардко	op"				
	Сертификаты IPsec	Запрещён доступ 14:21:44	на habr.com с адреса	192.168.17.4 по	ключевому сл	юву "мда"					
<b>Å</b>		Запрещён доступ 14:21:44	на cryptoworld.su c ад	peca 192.168.17	7.4 по ключево	ому слову "ba	ang"				
- <		« < Стр 1	из 1 →	>>			Показаны записи	1 - 13 из 13			

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

*	Защита	000 "Op	ганиза	ация" > Кон	тент-филь	тр 🕨 Событи	я	🚨 Адми	нистратор	£	≥ 35
<b>≗</b>	Антивирус ClamAV Антиспам Касперского	Контен	т-фил	њтр Нас	стройки	База контен	нт-фильтра	События	а Журна.	л	
	Антивирус Касперского Веб-фильтр Касперского			01.11.2019	- 01.11.2019	Сегодня	Неделя	Месяц	Другой пер	оиод 👻	C
•	Веб-фильтр SkyDNS	🛓 Эксп	орт						Поиск		Q
	Межсетевой экран Web Application Firewall	2000000		un un c7 addtl		100 140 1 <sup>°</sup>	7.4 50 (19)000		~ <sup>11</sup>		
õ	Application Firewall Летектор атак Suricata	URL:https://	н дост s7.addth	is.com/l10n/clien	it.ru.min.json	Jeca 192.100.1	7.4 IIO KJIKHEB	ому слову хх	X		
J	DLP	Запрещён 14:21:52	н дост	уп на apptract	tor.ru с адре	ca 192.168.17.4	1 по ключевом	ıy слову "banı	g"		
۶	Контент-фильтр Fail2ban	Запрещён 14:21:49	н дост	уп на edu.dev	todev.com c	адреса 192.16	8.17.4 по ключ	евому слову	"strip"		
	Сертификаты	Запрещён 14:21:44	н дост	уп на tproger.	ru с адреса (	192.168.17.4 no	о ключевому о	лову "хардко	p"		
	IPsec	Запрещён 14:21:44	н дост	уп на habr.cor	m с адреса 1	92.168.17.4 по	ключевому с.	пову "мда"			
*		Запрещён	н дост	уп на cryptow	/orld.su с адр	eca 192.168.1	7.4 по ключев	ому слову "ba	ing"		
<		<< <	Стр	1	из1 →	>>			Показаны заг	иси 1 - 1	.3 из 13

Для поиска по событиям есть поисковое поле.

**Важно.** Кнопка «Удалить логи» удаляет все логи, которые ведутся модулем «Контентфильтр».

## 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.

*	Защита	ООО "Организация"	<ul> <li>Контент-фильт</li> </ul>	р 🕨 Журнал	🚨 Админ	истратор 🚉	<b>5</b> 16
•	Антивирус ClamAV						
	Антиспам Касперского	Контент-фильтр	Настройки	База контент-фильтра	События	Журнал	
<b>m</b>	Антивирус Касперского	04.4	4 0040 04 44 0040	C	Manage		~
<b>O</b>	Веб-фильтр Касперского	01.1	1.2019 - 01.11.2019	Сегодня неделя	месяц	другой период 👻	Ũ
	Веб-фильтр SkyDNS	土 Экспорт Уда	алить логи		Г	Тоиск	Q
_	Межсетевой экран						
	Web Application Firewall						<b>↓</b> ↑
Ô	Application Firewall	Download finished					
,	Детектор атак Suricata	Lindata dana Currantu	version base 0.00				
۳	DLP	16:05:17	version base 7.00				
۶	Контент-фильтр	started					
	Fail2ban	ebus client [cf] connect	ted				
	Сертификаты	16:05:19					
	IPsec	exited 16:05:20					
		started 16:05:20					
		ebus client [cf] connect	ted				
٠							
<		« < Стр 1	из 1 🔷	»		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 «Контентфильтр».

#### From: https://doc-old.a-real.ru/ - Документация

Permanent link: https://doc-old.a-real.ru/doku.php?id=ics70:content&rev=1585122040



Last update: 2020/03/25 10:40