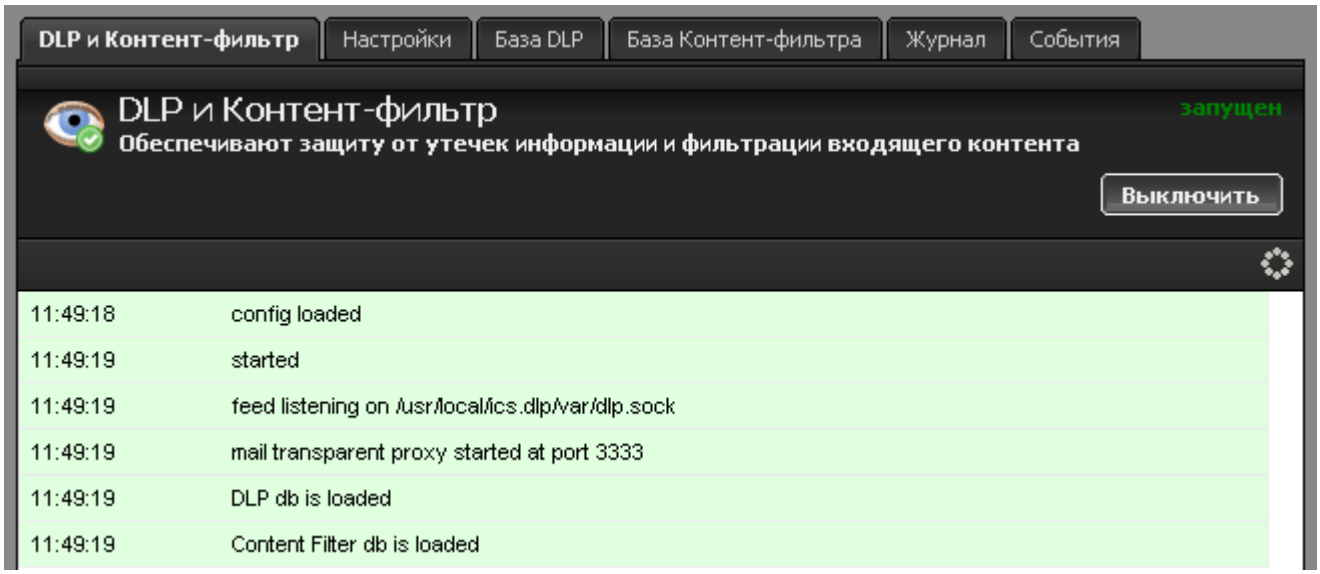
DLP и контент-фильтр

Общие сведения

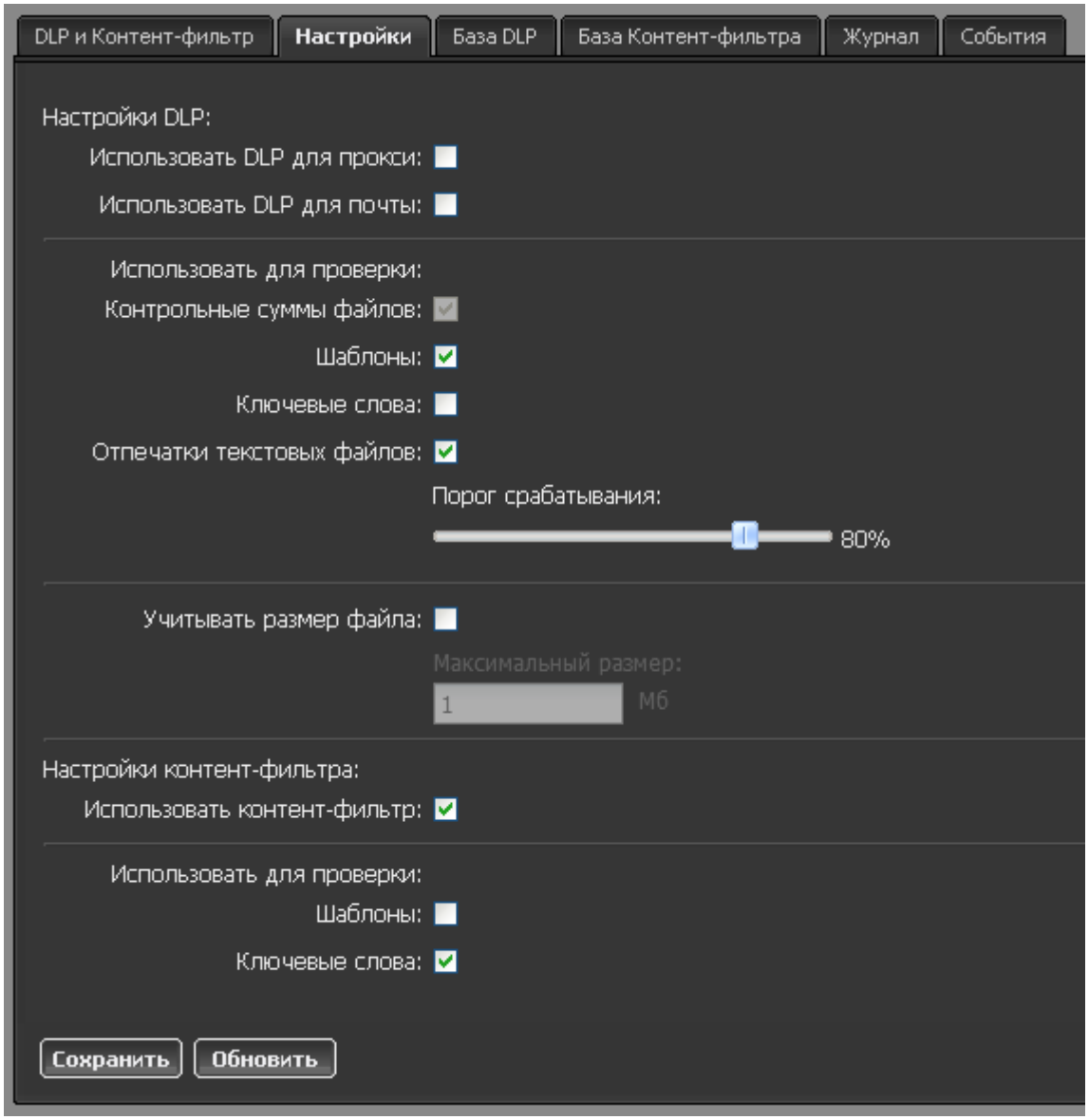
DLP (Data Leak Prevention) — технология предотвращения утечек конфиденциальной информации из внутренней сети. DLP-система базируется на анализе потоков данных, проходящих через шлюз сети. При обнаружении конфиденциальной информации срабатывает защита, и передача блокируется.



При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

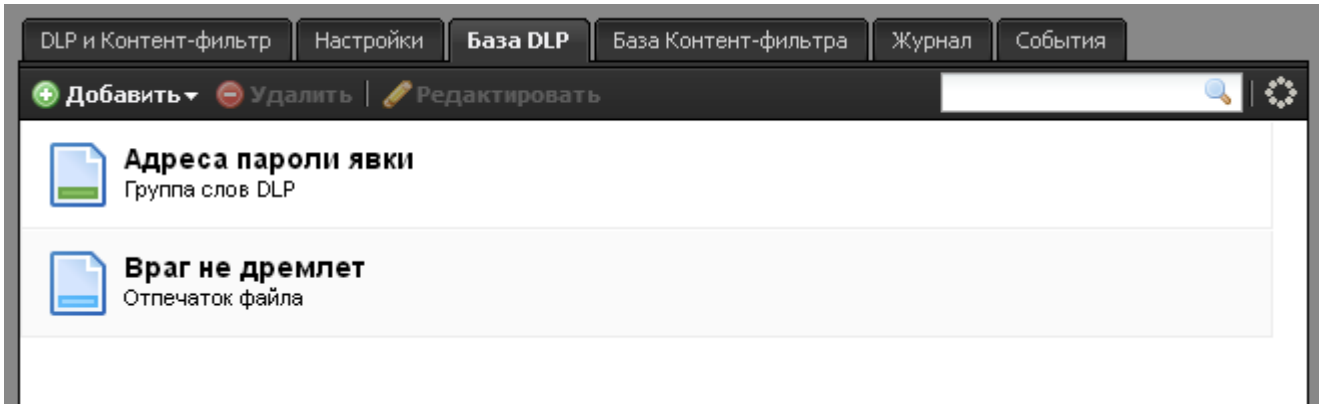
Настройки

Модуль DLP проверяет отпечатки в почтовых сообщениях ИКС и в HTTP-трафике. Чтобы начать активную проверку, отметьте флажками одну или обе из возможностей работы.

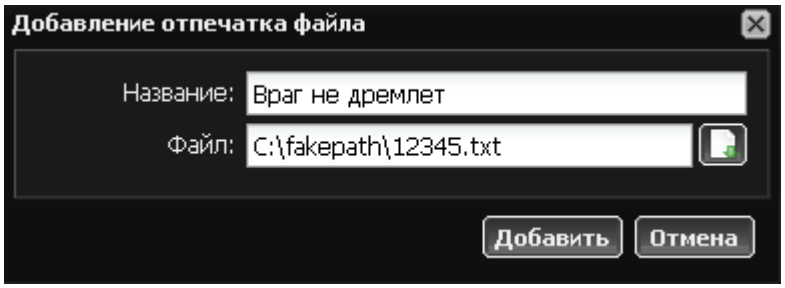


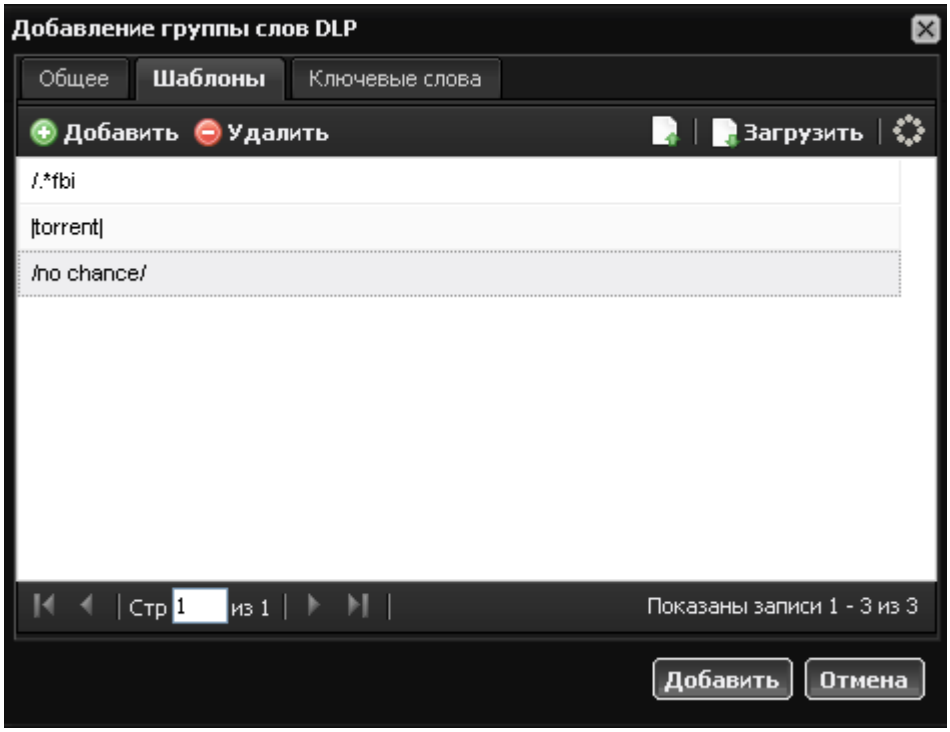
Дальнейшие параметры позволяют определить, по каким критериям определять конфиденциальность информации, а также порог срабатывания. При необходимости, вы можете определить максимальный размер обрабатываемого файла, что позволит снизить нагрузку модуля на систему. Также, настройки позволяют задействовать контент-фильтр для работы с пользователями и определить данные, используемые для проверки. Отключение одного из видов данных (шаблоны и ключевые слова) позволяет снизить нагрузку на систему.

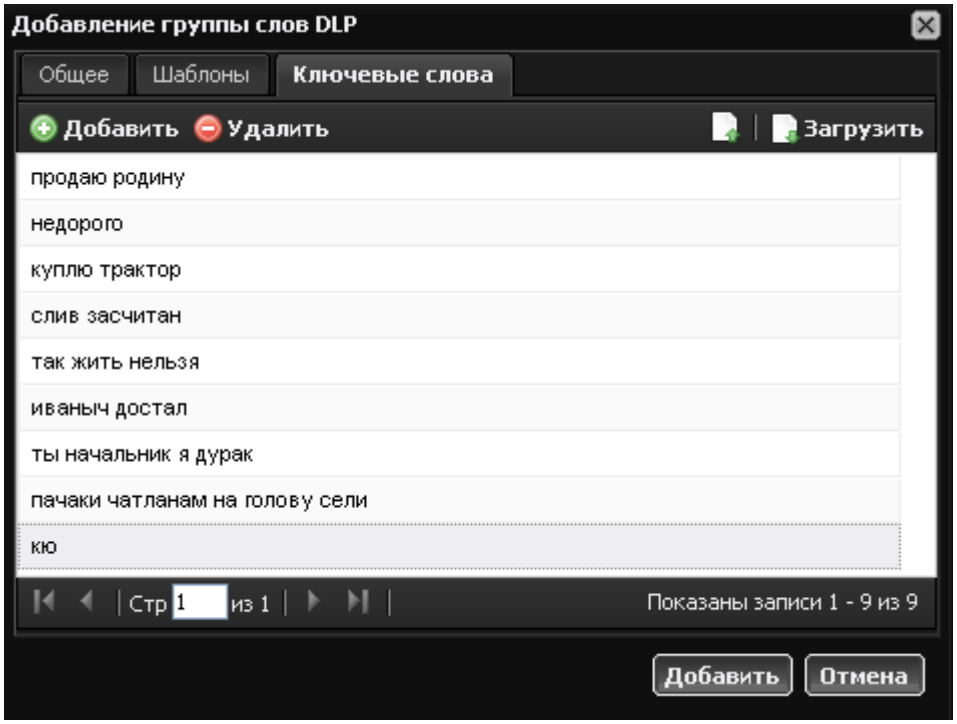
База DLP



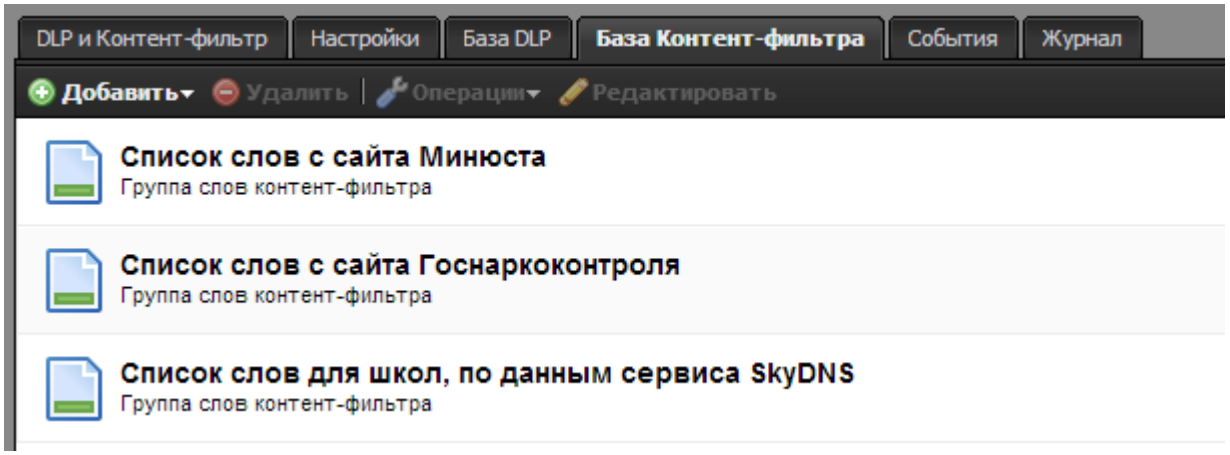
В следующей вкладке вы можете создать список отпечатков по файлам и ключевым словам, согласно которому будет происходить проверка. В список ключевых слов также входят шаблоны, которые состоят из регулярных выражений аналогично правилам прокси.





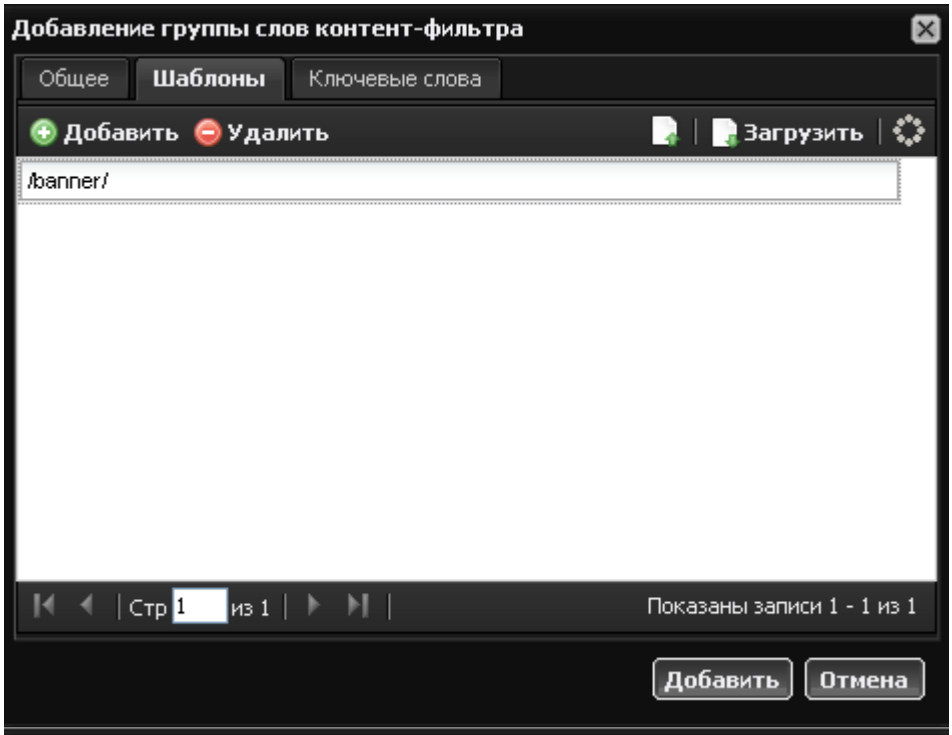


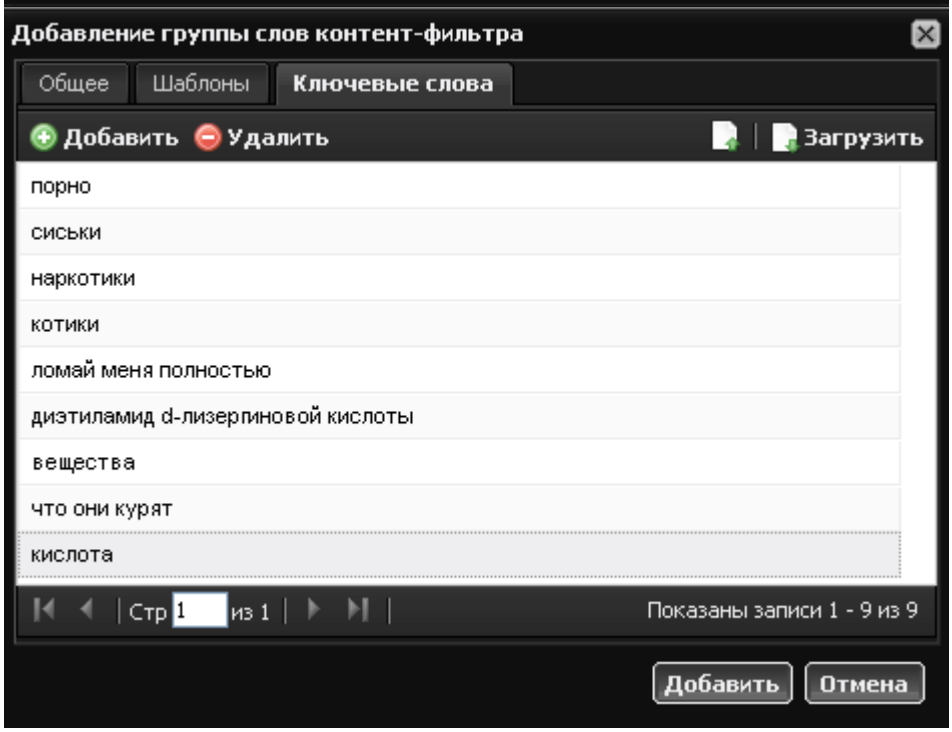
База контент-фильтра



Контент-фильтр позволяет настроить правила пользователей на блокировку интернет-страниц, если в их HTML-коде содержатся заданные ключевые слова или регулярные выражения.

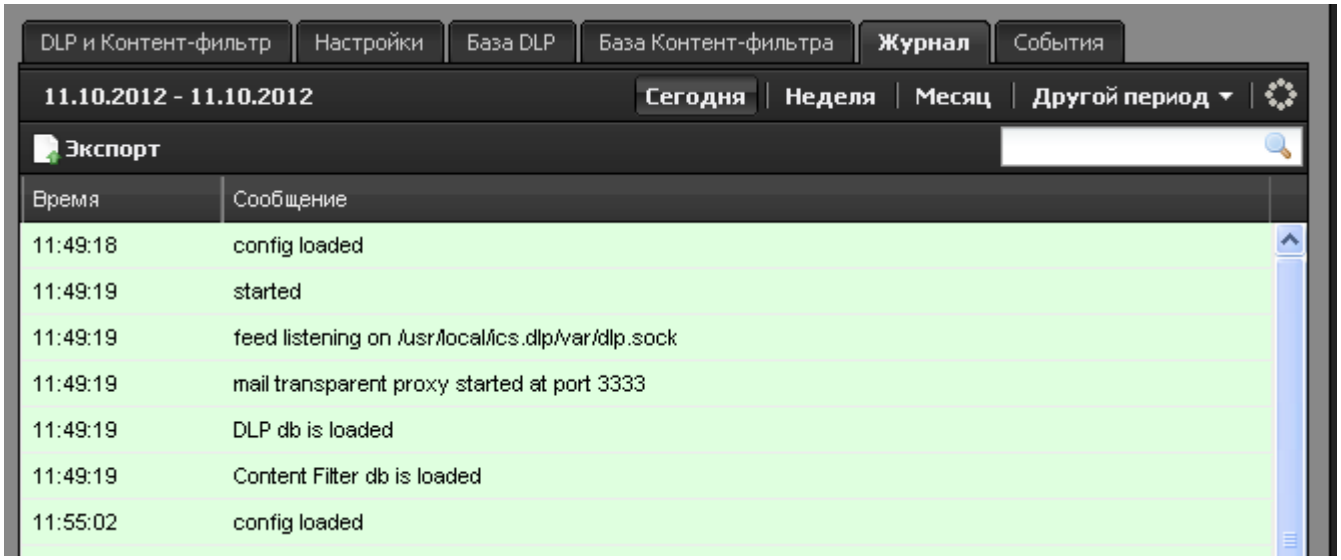
По умолчанию база контент-фильтра уже содержит список слов, запрещенных Минюстом и Госнаркоконтролем, а также специальный список облачного сервиса SkyDNS. Следует учесть, что контент-фильтр обращается ко всей базе целиком.





После добавления объектов DLP и контент-фильтрации, вы можете назначить их нужным пользователям или группам через правила и ограничения.

Журнал



В закладке «Журнал» находится сводка всех системных сообщений модуля. По структуре он аналогичен журналам других служб.

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

Permanent link:
https://doc-old.a-real.ru/doku.php?id=en:dlp

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