DLP

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

Флаги **Использовать DLP для прокси** и **Использовать DLP для почты** соответствуют аналогичным флагам в разделах «Прокси» и «Почта», при их установке модуль DLP проверяет отпечатки в почтовых сообщениях ИКС и в HTTP-трафике.

Флаги **Контрольные суммы файлов**, **Шаблоны**, **Ключевые слова**, **Опечатки текстовых файлов** позволяют определить, по каким критериям определять конфиденциальность информации, а также порог срабатывания для последнего.

Флаг **Учитывать размер файла** определяет максимальный размер обрабатываемого файла, что позволит снизить нагрузку модуля на систему.

Флаг **Использовать внешний DLP сервер** дает возможность указать внешний сервер проверки.

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.

События

Вкладка «События» содержит список всех блокировок DLP. В каждой строке блокировки указан пользователь, для которого был заблокирован ресурс, а также причина блокировки.

Журнал

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