DLP

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.

Модуль «DLP» расположен в Меню «Защита». Данный модуль предназначен для блокировки передачи конфиденциальной информации. Модуль «DLP» имеет пять вкладок: «DLP», «Настройки», «База DLP», «События» и «Журнал».

Общие сведения

Вкладка «DLP». На данной вкладке отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Настройки

Вкладка «Настройки». Данная вкладка предназначена для настройки работы модуля «DLP».

Флаги **Использовать DLP для прокси** и **Использовать DLP для почты** соответствуют аналогичным флагам в разделах настроек модулей «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

Вкладка «База DLP». Данная вкладка предназначена для управления списком файловых отпечатков и групп слов, согласно которому будет происходить проверка.

Отпечаток файла

Объект «Отпечаток файла» предназначен для защиты от передачи конкретного файла. Для добавления отпечатка файла необходимо нажать «Добавить» - «Отпечаток файла», откроется диалоговое окно, в котором будет предложено выбрать файл и дать описание отпечатку (по умолчанию, поле будет заполнено именем выбранного файла).

После добавления отпечатка он будет загружен в асинхронном режиме, а в списке базы DLP отобразятся проценты загрузки.

Группа слов DLP

Объект «Группа слов DLP» предназначен для защиты от передачи текстового файла с соответствующим содержимым. Для добавления группы слов необходимо нажать «Добавить» - «Группа слов DLP», откроется диалоговое окно с тремя вкладками: «Общее», «Шаблоны» и «Ключевые слова», при этом активна будет вкладка «Общее».

Вкладка «Общее». Для создания объекта будет предложено ввести «Название» (Обязательный параметр) и «Описание» (не обязательный параметр).

Вкладка «Шаблоны». Эта вкладка предназначена для добавления словосочетаний и регулярных выражений. При указании в этом списке отдельного слова, система будет искать его в других словах как комбинацию символов.

Вкладка «Ключевые слова». Эта вкладка предназначена для добавления отдельных слов.

Если необходимо сохранить список используемых правил, то в каждой вкладке есть функция экспорта в текстовый файл. Также реализована обратная функция, если есть файл, в формате *.txt, то его можно импортировать нажав на кнопку «Импорт».

События

Вкладка «События». Данная вкладка содержит список всех блокировок DLP. В каждой строке

блокировки указан пользователь либо ip-адрес, для которого был заблокирован ресурс, а также причина блокировки (название отпечатка или группа слов).

Журнал

Вкладка «Журнал». Отображает сводку всех системных сообщений модуля «DLP» с указанием даты и времени. Журнал разделен на страницы, кнопками «вперед» и «назад» возможно переходить со страницы на страницу, либо ввести номер требуемой страницы. Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение) - зеленым, предупреждения – желтым, ошибки - красным. 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».