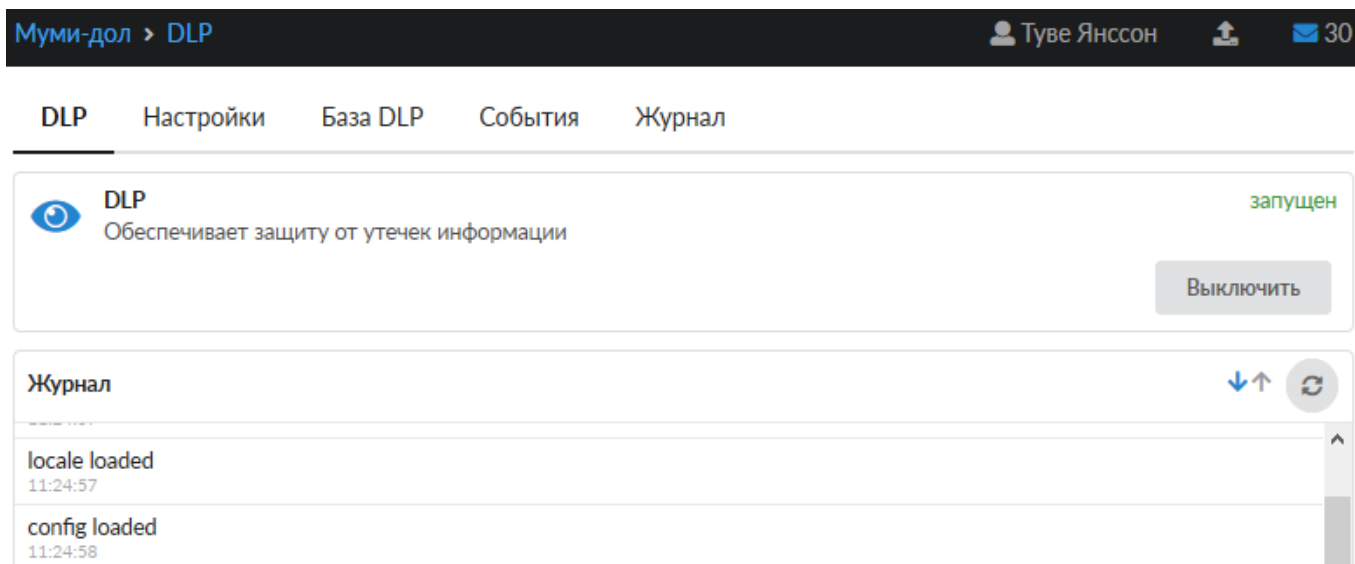




# DLP

**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



Муми-дол > DLP Тове Янссон   30

DLP    Настройки    База DLP    События    Журнал

**DLP** запущен  
Обеспечивает защиту от утечек информации Выключить

**Журнал** ↓↑ 

locale loaded  
11:24:57

config loaded  
11:24:58

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

## Настройки

DLP   **Настройки**   База DLP   События   Журнал

---

Использовать DLP для прокси

Использовать DLP для почты

---

Использовать для проверки:

Контрольные суммы файлов

Шаблоны

Ключевые слова

Отпечатки текстовых файлов

80   ^   %  
v

**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**, **Отпечатки текстовых файлов** позволяют определить, по каким критериям определять конфиденциальность информации, а также порог срабатывания для последнего.

---

Учитывать размер файла

1   ^   Мб  
v

---

Использовать внешний DLP сервер

Сервер	Порт
(не использовать)	1344

---

**Сохранить**   Обновить

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

DLP    Настройки    **База DLP**    События    Журнал

Добавить ▾    Удалить    Выключить    Редактировать

Поиск... 🔍 ↻

	<b>Ключ сертификата для муми-сети</b> Отпечаток файла
	<b>Приветствие</b> Отпечаток файла
	<b>Запрещено к передаче</b> Группа слов DLP Королевский рубин, Одинокие горы, Шляпа волшебника барометр, ботаник, грот, пещера

Удалить    Редактировать    Выключить

**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).

### Добавление отпечатка файла

Название \*

Файл \*

**Добавить**    Отмена

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».

### Добавление группы слов DLP

Общее   Шаблоны   Ключевые слова

---

Название \*      Описание



Запрещено к передаче      Описание

Добавить      Отмена

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

Общее    Шаблоны    Ключевые слова

---



Добавить    Удалить     Импорт      3 записи 

Шляпа волшебника
Королевский рубин
Одинокие горы

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.

Общее   Шаблоны   **Ключевые слова**

---

**Добавить**   Удалить    Импорт   4 записи 

грот
барометр
ботаник
пещера


**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

DLP   Настройки   База DLP   **События**   Журнал

---

08.11.2019 - 08.11.2019   **Сегодня**   Неделя   Месяц   Другой период ▾   

 Экспорт   Поиск... 

Запрещена отправка письма от mama@mumi.dol для daddy@mumi.dol 11:58:09
Запрещена передача файла "goose2.png" от 192.168.17.43 Файл: "goose2.png" URI: https://drive.google.com Совпадение по: отпечатку  Galactic guardian goose (контрольная сумма) 12:25:17

**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

DLP    Настройки    База DLP    События    **Журнал**

08.11.2019 - 08.11.2019    **Сегодня**    Неделя    Месяц    Другой период ▾    ↻

↑ Экспорт    Удалить логи    Поиск...    🔍

started 11:24:57
locale loaded 11:24:57
config loaded 11:24:58
mail transparent proxy started at port 3333 11:24:58
DLP db is loaded 11:24:58

**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».

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

Permanent link:  
<https://doc.a-real.ru/doku.php?id=ics70:dlp>

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

