Yara

Страница, на которой отображается список yara-сигнатур. YARA сигнатуры могут быть использованы для обнаружения известных вредоносных программ, вредоносных поведенческих шаблонов и их классификации.

Существует обязательный список сигнатур от вендора, подсвеченных серым цветом.

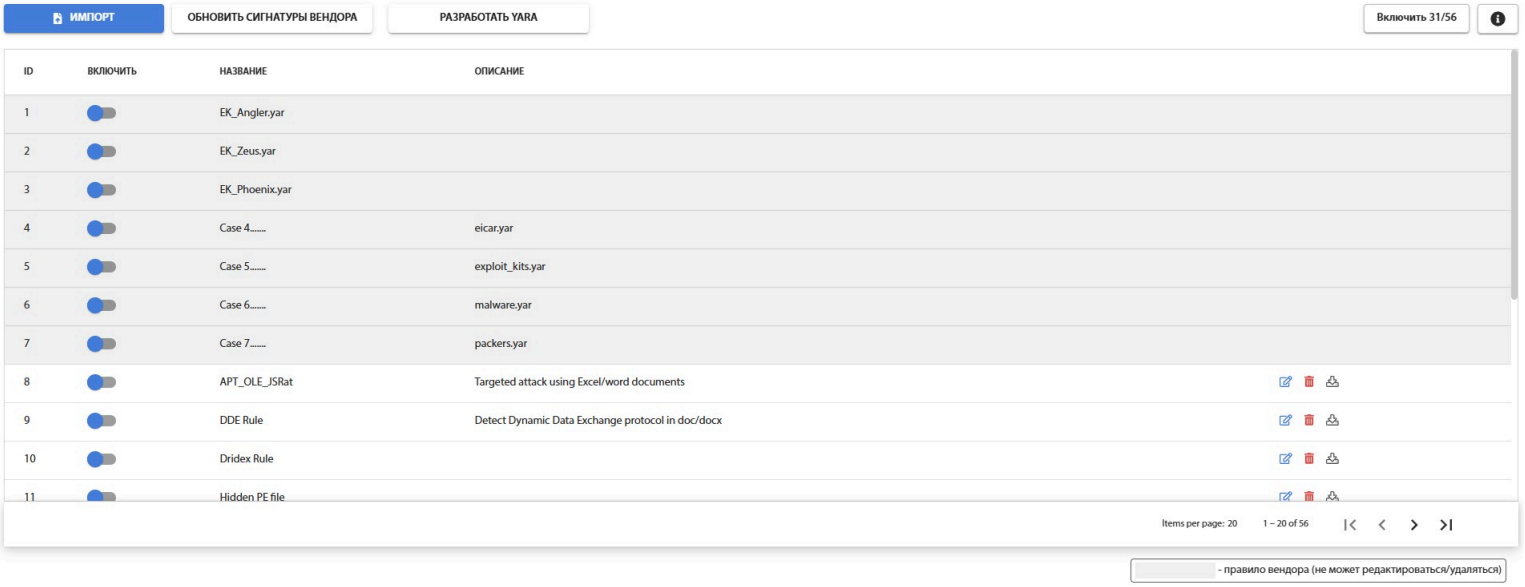

Рис. 4.6.1 - таблица yara-сигнатур

Нажав на кнопку  , можно открыть окно с подробной информацией о модулях и другое.

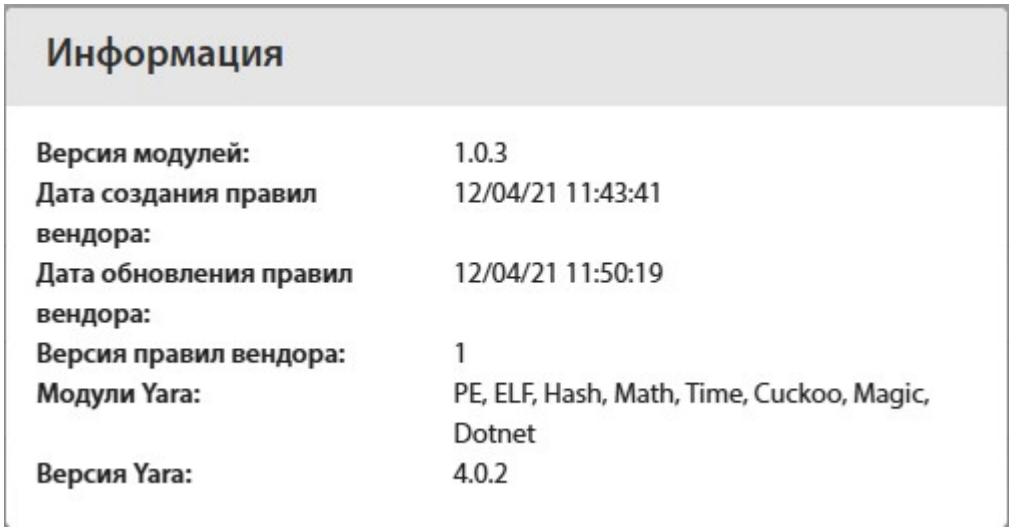

Рис. 4.6.2 - окно с подробной информацией о Yara

Кнопка ⬇ позволяет скачать Yara-сигнатру файлом формата .yara.

Импорт правила осуществляется кнопкой 

Для импорта нужно указать путь к файлу формата ".yara", название и описание. Сигнатуры вендора доступны к обновлению только через системный функционал с помощью кнопки **ОБНОВИТЬ СИГНАТУРЫ ВЕНДОРА**. На вход подается архивный файл с сигнатурами.