Руководство администратора

Table of contents:

Руководство администратора

Пользовательские и системные настройки

Кнопка с именем пользователя в верхнем навигационном меню открывает меню настроек.

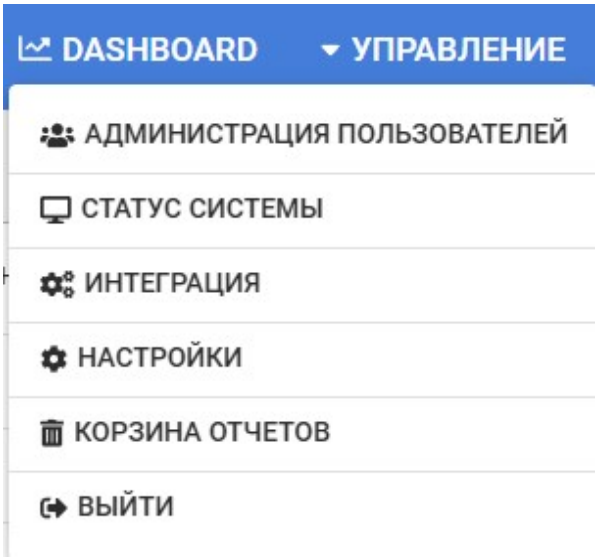


Рис. 1 - Меню настроек

Администрирование пользователей

Отображает список всех пользователей. В данном разделе можно создать нового пользователя (Добавить учетную запись), сменить пароль существующему (Поменять пароль), посмотреть отчеты, принадлежащие пользователям (нажать на логин пользователя).

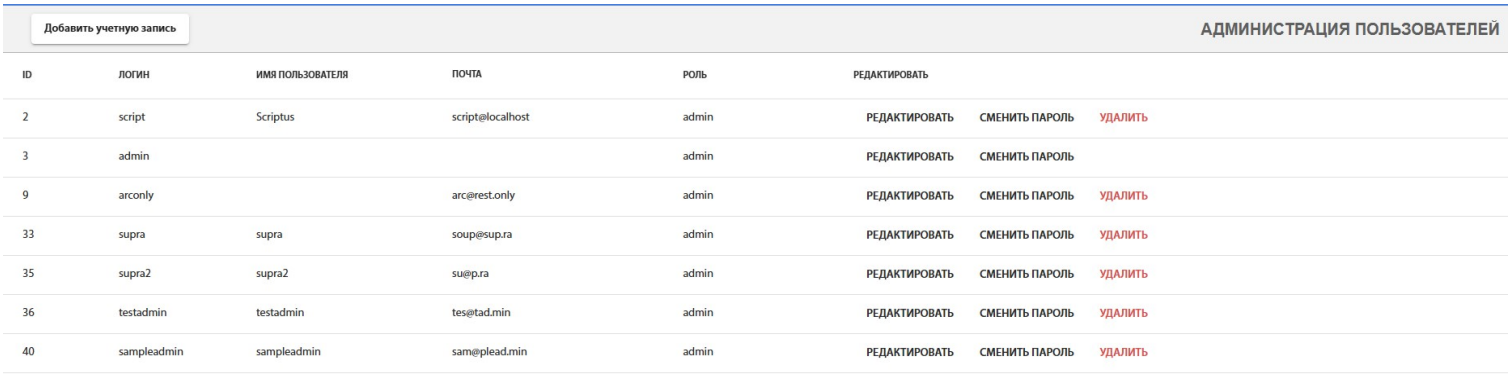


Рис 2.1 - таблица пользователей

Смена пароля пользователя

Смена пароля пользователя производится при нажатии кнопки "Сменить пароль" в соответствующем данному пользователю столбце в таблице. При нажатии кнопки, открывается модальное окно, в котором нужно задать новый пароль

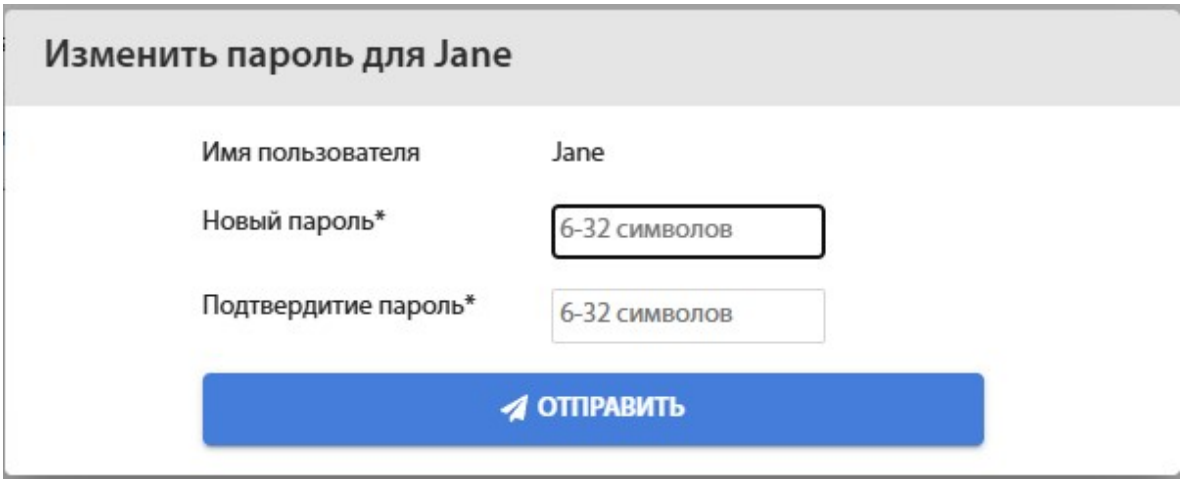


Рис. 2.2 - окно смены пароля

Создание новых пользователей

Создание новых учетных записей производится администратором на странице "Администрация пользователей" в верхнем правом меню. "Добавить учетную запись" открывает форму для создания нового пользователя. Электронная почта, логин и пароль являются обязательными полями. Пользователь может самостоятельно изменить свой пароль.

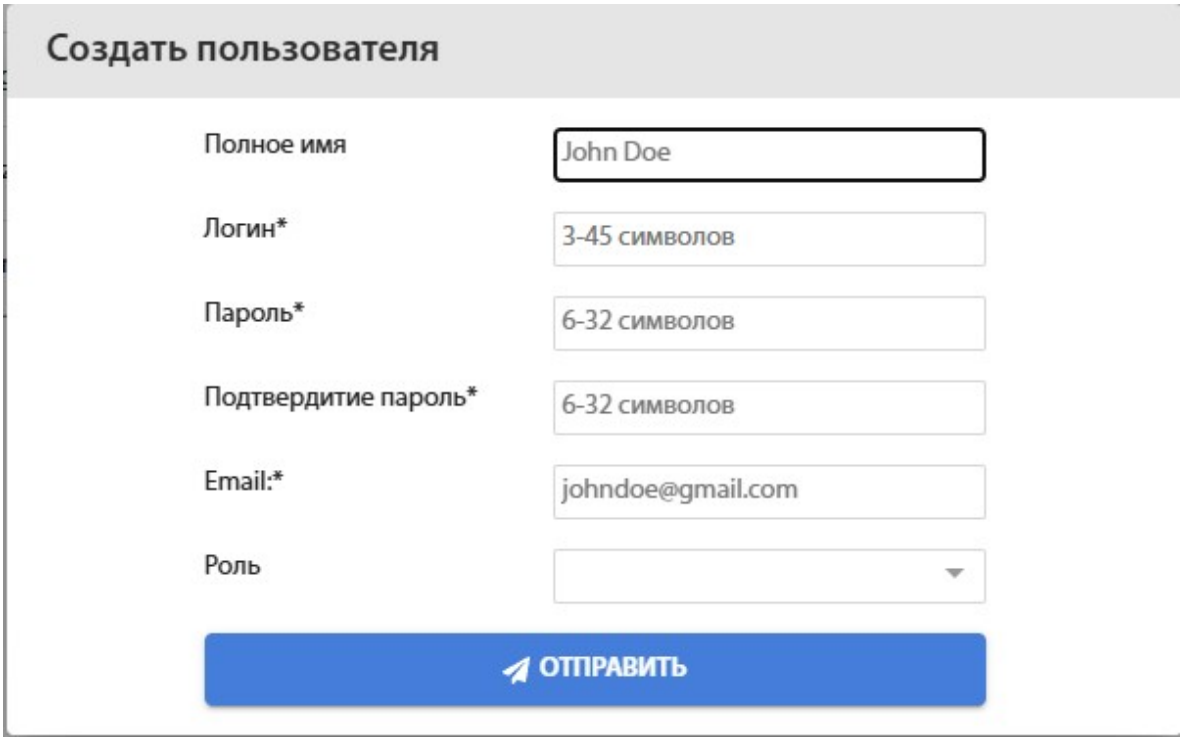


Рис. 2 - форма создания нового пользователя

Редактирование пользователей

Редактирование данных пользователя производится при нажатии кнопки "Редактировать" в соответствующем данному пользователю столбце в таблице. Принажатии кнопки, открывается модальное окно, в котором нужно задать новые данные.

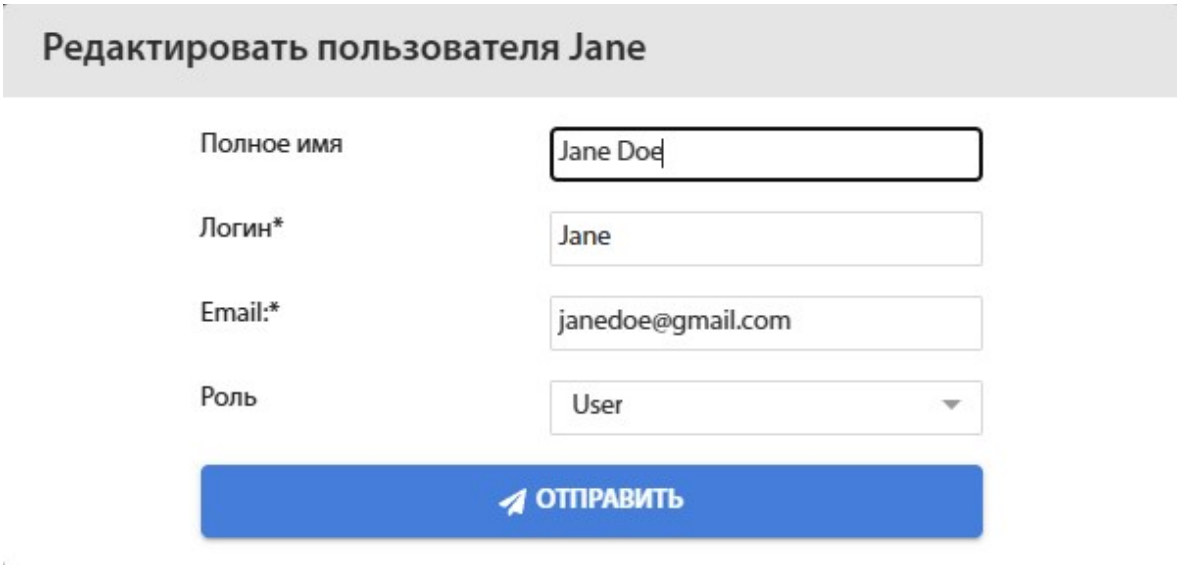


Рис. 2.3 - окно редактирования пользователя

Роли пользователей

Система поддерживает следующие роли пользователей: обычный пользователь, эксперт и администратор.

В режиме обычного пользователя предоставляются следующие возможности: загрузка файлов для анализа и просмотр отчетов по загруженным файлам. Обычным пользователям видны собственные отчеты и отчеты с открытым доступом.

В режиме эксперта обеспечена возможность для установки вердикта проанализированных объектов, а также все возможности обычного пользователя.

У пользователя системы с ролью администратора присутствуют возможности эксперта и обычного пользователя, а также панель настройки параметров компонентов и управление пользователями. Администратору видны отчеты всех пользователей.

Среда исполнения

Эта страница отображает статус среды исполнения и всех виртуальных машин в ней, статус аппаратных ресурсов, а ...

Аппаратные ресурсы

Страница, показывающая статус аппаратных ресурсов системы в виде интерактивных графиков с возможностью из...

Службы tLab

Компонент, показывающий статусы и логи служб, функционирующих в системе. Статус может быть «АКТИВНЫЙ» ил...

Среда исполнения

Эта страница отображает статус среды исполнения и всех виртуальных машин в ней, статус аппаратных ресурсов, а также служб tLab. Перед использованием динамического анализа среда должна быть включена. Если статус машины горит желтым цветом с названием «ЗАРЕЗЕРВИРОВАНА», то на данной машине выполняется анализ файла. Кликнув на название отчета под заголовком «Задание», можно перейти на данный отчет.

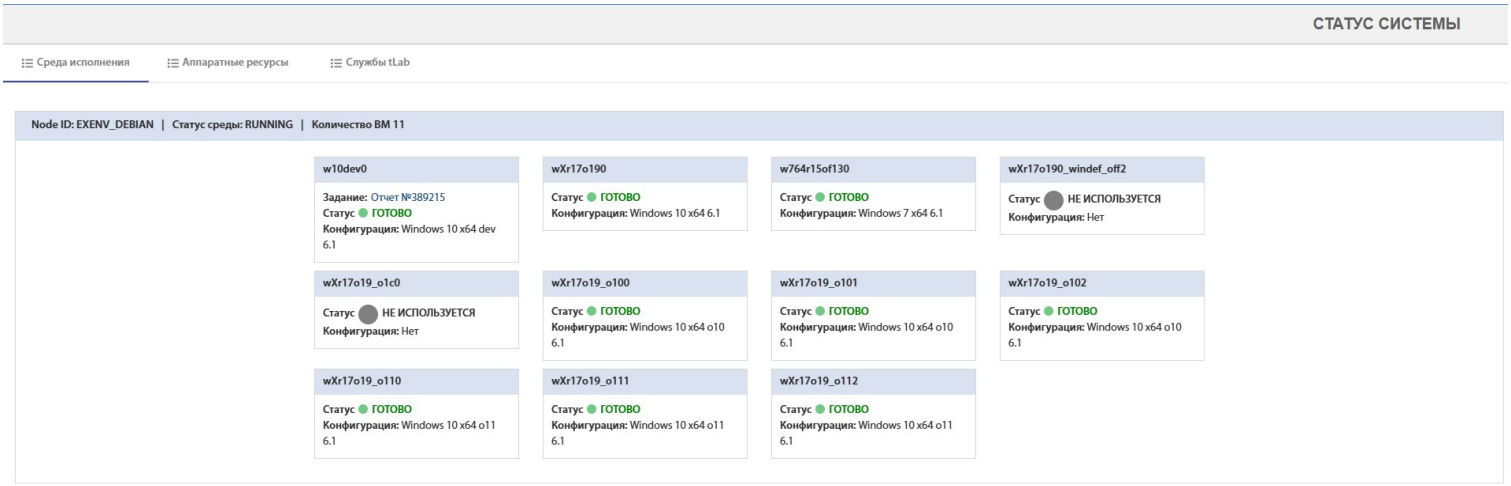


Рис. 3 - Страница управления

Аппаратные ресурсы

Страница, показывающая статус аппаратных ресурсов системы в виде интерактивных графиков с возможностью изменения периода времени. Информация, доступная для просмотра: физические диски, использование диска,логические диски, память, процессорное время, сетевые интерфейсы, средняя нагрузка процессоров.

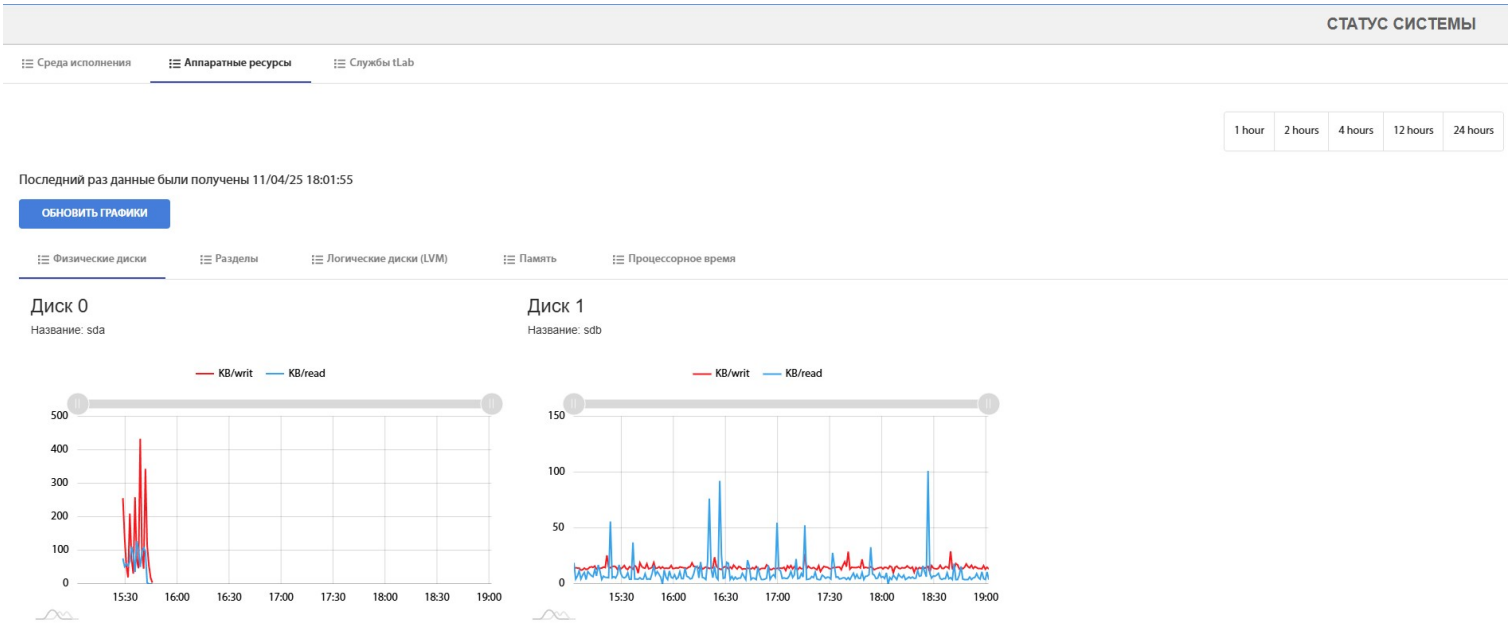


Рис. 3.1 - Страница аппаратных ресурсов

Службы tLab

Компонент, показывающий статусы и логи служб, функционирующих в системе. Статус может быть «АКТИВНЫЙ» или «НЕАКТИВНЫЙ».

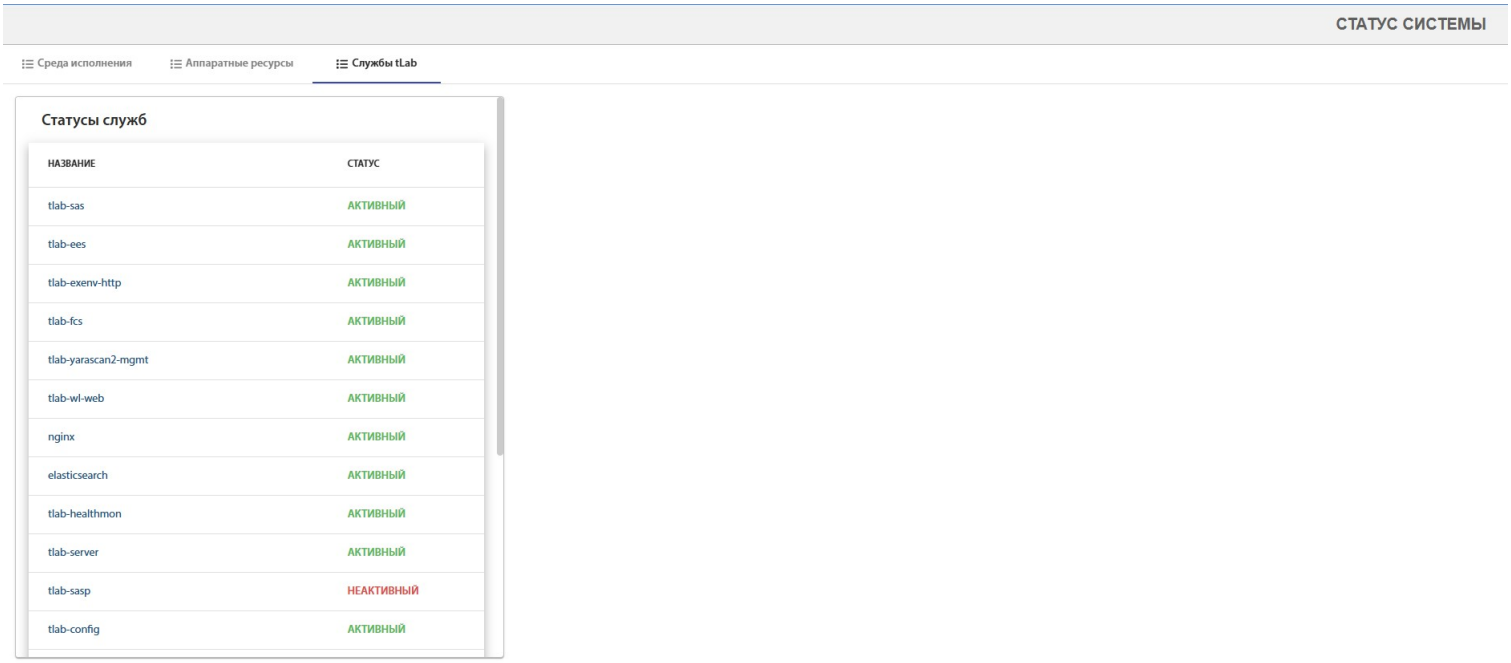


Рис 3.2 - Страница служб tLab

Настройки

На данной странице настраиваются различные свойства системы.

Максимальный размер загрузки - максимальный общий объем файлов, отправляемых на анализ.

Задержка исполнения - указывается минимальное время задержки прикотором будет обнаруживаться задержка как подозрительное событие исоответственно включаться противодействие.

Автоматическое экспертное заключение - позволяет настроить уровень опасности, при котором файл будет иметь заключение эксперт: Опасно.

Противодействия методам уклонения ВПО - дает возможность выбора методапротиводействия задержке исполнения (исключить задержку - задержки не будет; уменьшить задержку в n раз - идет перехват функции задержки и ее сокращения в n раз).

Типы файлов допустимых к анализу - дает возможность запретить анализ определенных типов файлов. После изменения свойства необходимо нажать кнопку "Применить изменения" внутри панели этого свойства для сохранения.

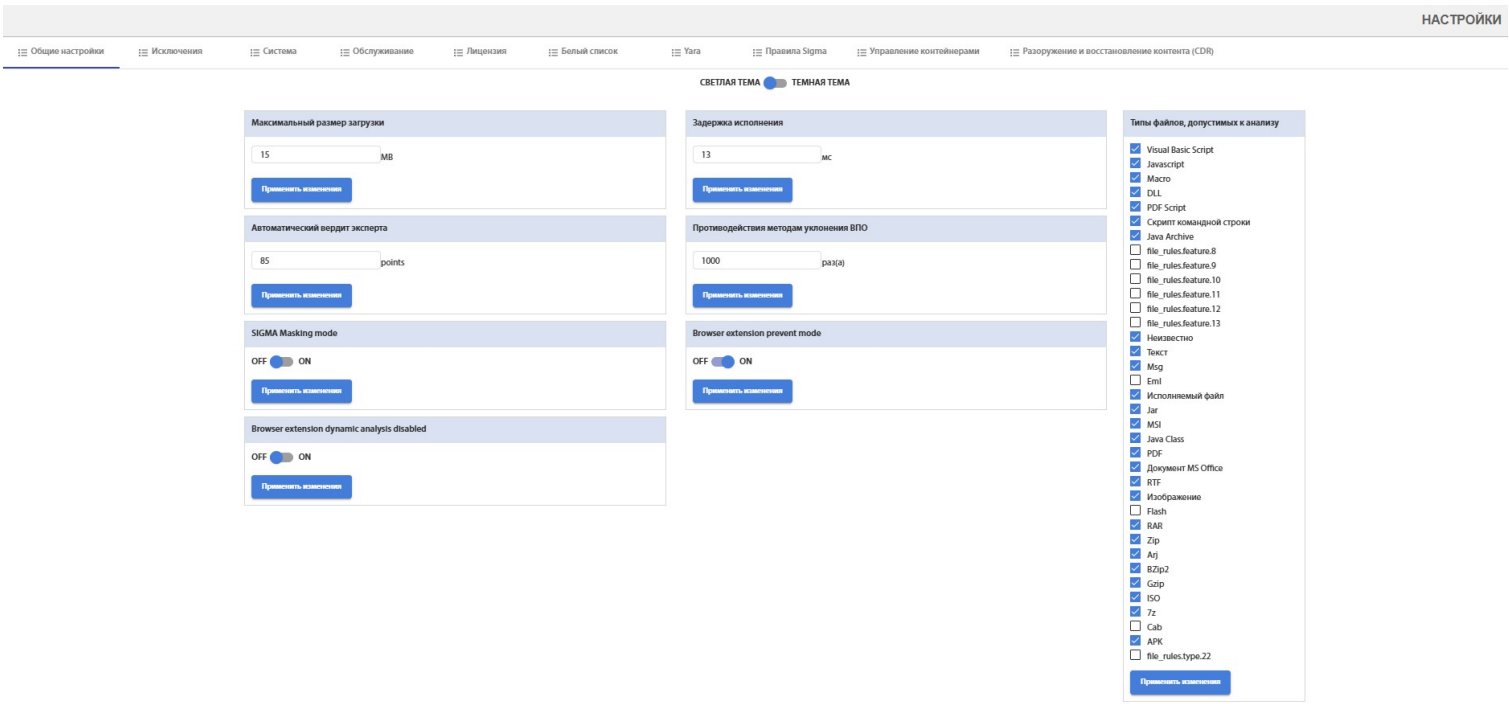


Рис. 4 - Страница настроек системы

Исключения

Таблица со списком добавленных ранее исключений (файлов или директорий). Позволяет редактировать исключения, а также включать или выключать их.

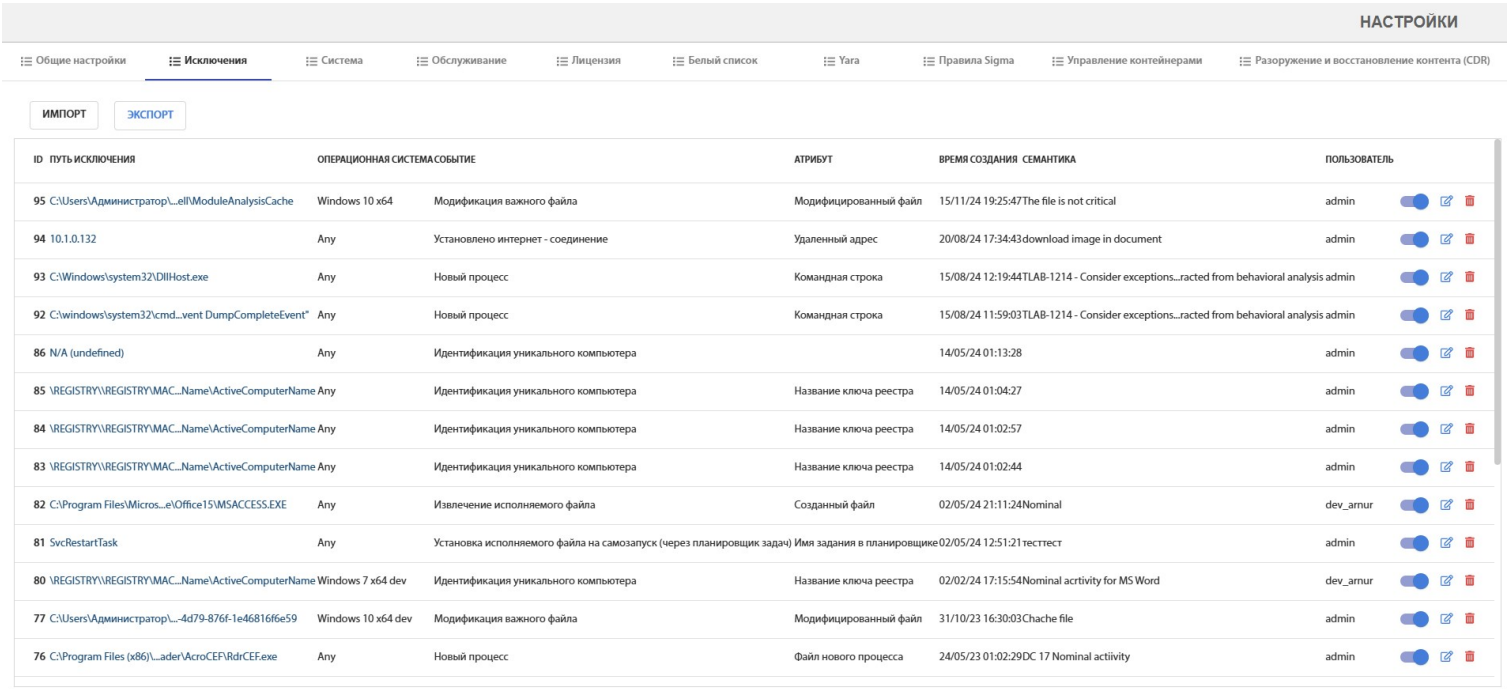


Fig. 4.1 – Страница исключений

Управление исключением

Включение/выключение исключения производится с помощью кнопки - переключателя. Если исключение включено, то оно будет учитываться привычислении уровня угрозы файла.

Редактирование и удаление исключения выполняется с помощью кнопок в столбце: ввиде карандаша и корзины соответственно.

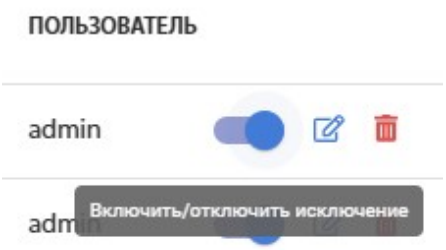


Рис 4.1.1 - кнопки управления исключением

Импорт / экспорт исключений

Для выполнения импорта исключений нужно нажать кнопку "Импорт". В открытом окне нужно выбрать файл формата json, который ранее экспортировался с системы. Итогом импорта будет добавление новых исключений, при этом старые останутся без изменения.

Для выполнения экспорта исключения нужно нажать на кнопку "Экспорт". Посленажатия будет скачан файл "exclusions.json"

Рис. 4.1.2 - кнопки импорта и экспорта списка исключений

Сеть

Позволяет применять настройки сети системы.

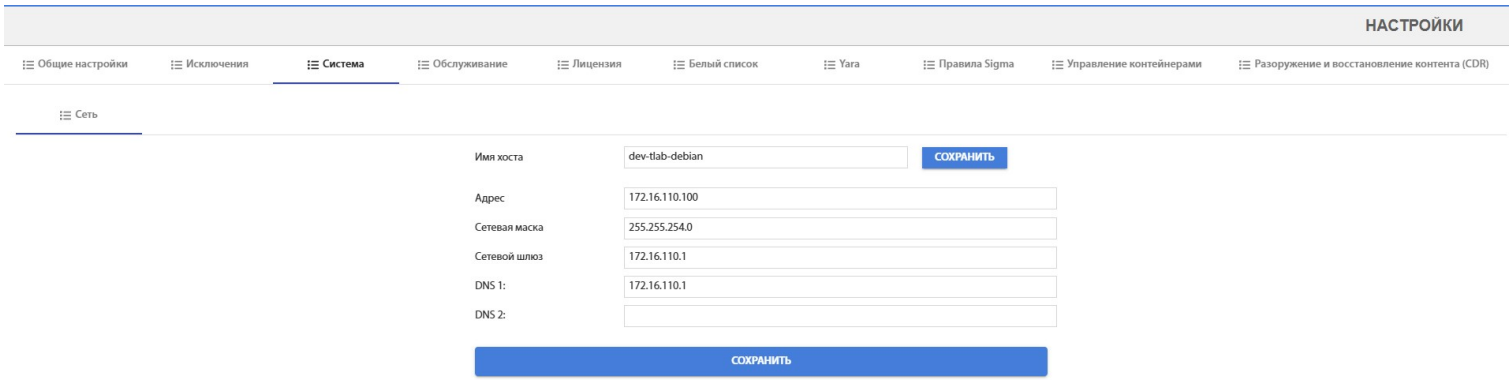


Рис 4.2 - Страница настроек сети

Обслуживание

Страница, на которой предоставляется возможность выключения или перезагрузки системы tLab. Перезагрузка может занимать несколько минут.

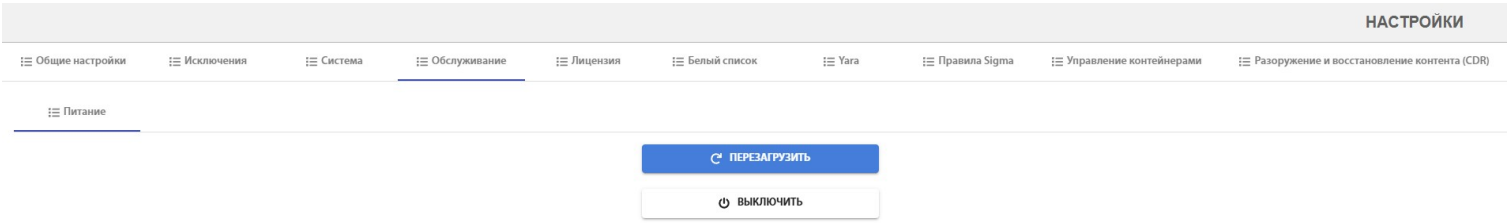


Рис 4.3 - Страница обслуживания системы

Лицензия

Страница, на которой присутствует базовая информация о лицензии и полеактивации лицензии.

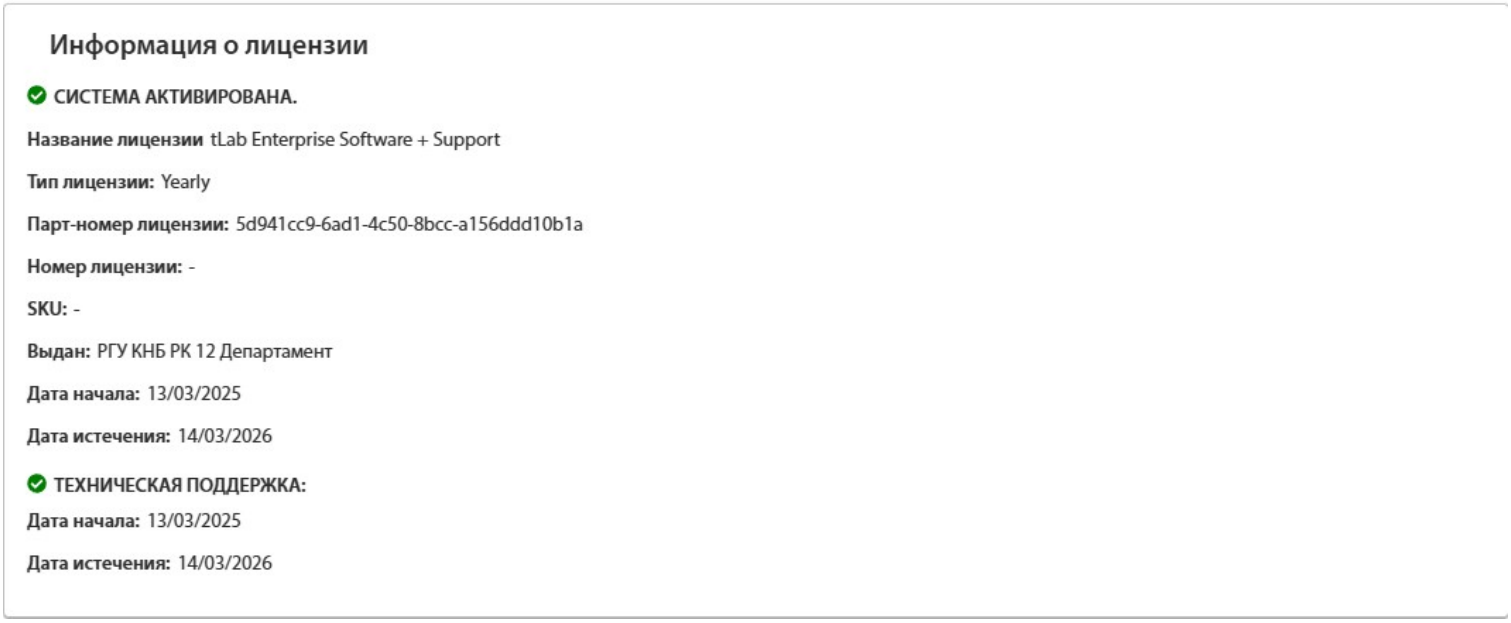


Рис. 4.4.1 - окно информации о лицензии

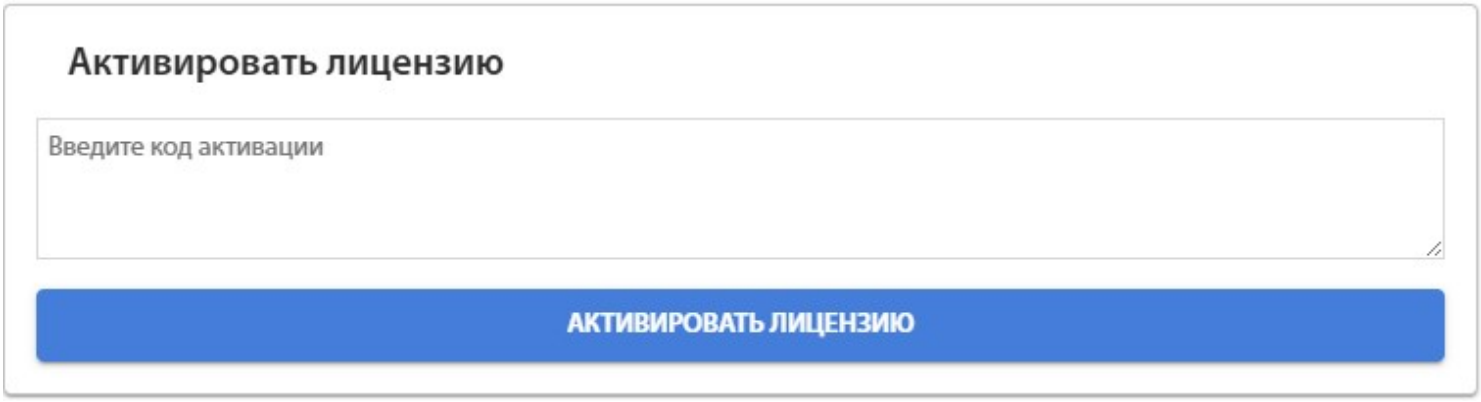
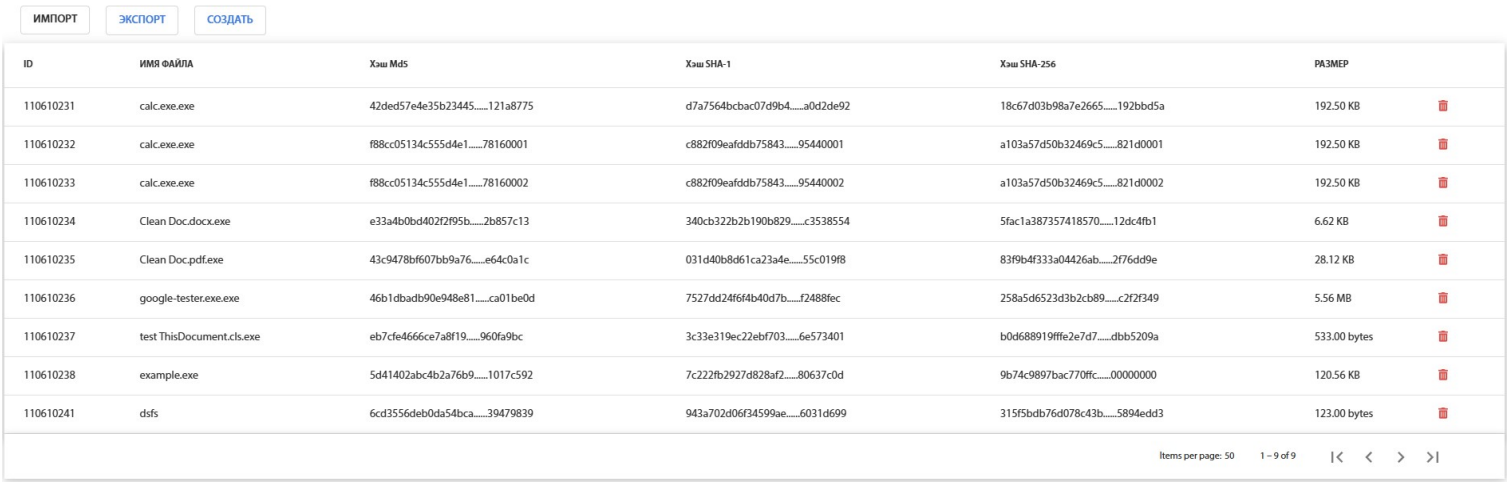


Рис. 4.4.2 - окно активации лицензии

Белый список

Страница, на которой отображается список доверенных файлов, которые система безопасности считает безопасными. Анализ файлов, включенных в данныйсписок, будет отклоняться со статусом WHITELISTED.



ID	ИМЯ ФАЙЛА	Хэш Md5	Хэш SHA-1	Хэш SHA-256	РАЗМЕР
110610231	calc.exe.exe	42ded57e4e35b23445.....121a8775	d7a7564bcbac07d9b4.....a0d2de92	18c67d03b98a7e2665.....192bbd5a	192.50 KB
110610232	calc.exe.exe	f88cc05134c555d4e1.....78160001	c882f09eafddb75843.....95440001	a103a57d50b32469c5.....821d0001	192.50 KB
110610233	calc.exe.exe	f88cc05134c555d4e1.....78160002	c882f09eafddb75843.....95440002	a103a57d50b32469c5.....821d0002	192.50 KB
110610234	Clean Doc.docx.exe	e33a4b0bd402f2f95b.....2b857c13	340cb322b2b190b829.....c3538554	5fac1a387357418570.....12dc4fb1	6.62 KB
110610235	Clean Doc.pdf.exe	43c9478bf607bb9a76.....e64c0a1c	031d40b8d61ca23a4e.....55c019f8	83f9b4f333a04426ab.....2f76dd9e	28.12 KB
110610236	google-tester.exe.exe	46b1dbadb90e948e81.....ca01be0d	7527dd24f6f4b40d7b.....f2488fec	258a5d6523d3b2cb89.....c2f2f349	5.56 MB
110610237	test ThisDocument.cls.exe	eb7cfe4666ce7a8f19.....960fa9bc	3c33e319ec22ebf703.....6e573401	b0d688919fffe2e7d7.....dbb5209a	533.00 bytes
110610238	example.exe	5d41402abc4b2a76b9.....1017c592	7c222fb2927d828af2.....80637c0d	9b74c9897bac770ffc.....00000000	120.56 KB
110610241	dsfs	6cd3556deb0da54bca.....39479839	943a702d06f34599ae.....6031d699	315f5bdb76d078c43b.....5894edd3	123.00 bytes

Рис. 4.5.1 - таблица белого списка

Добавление файлов в список производится путём импорта XML файла.

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.

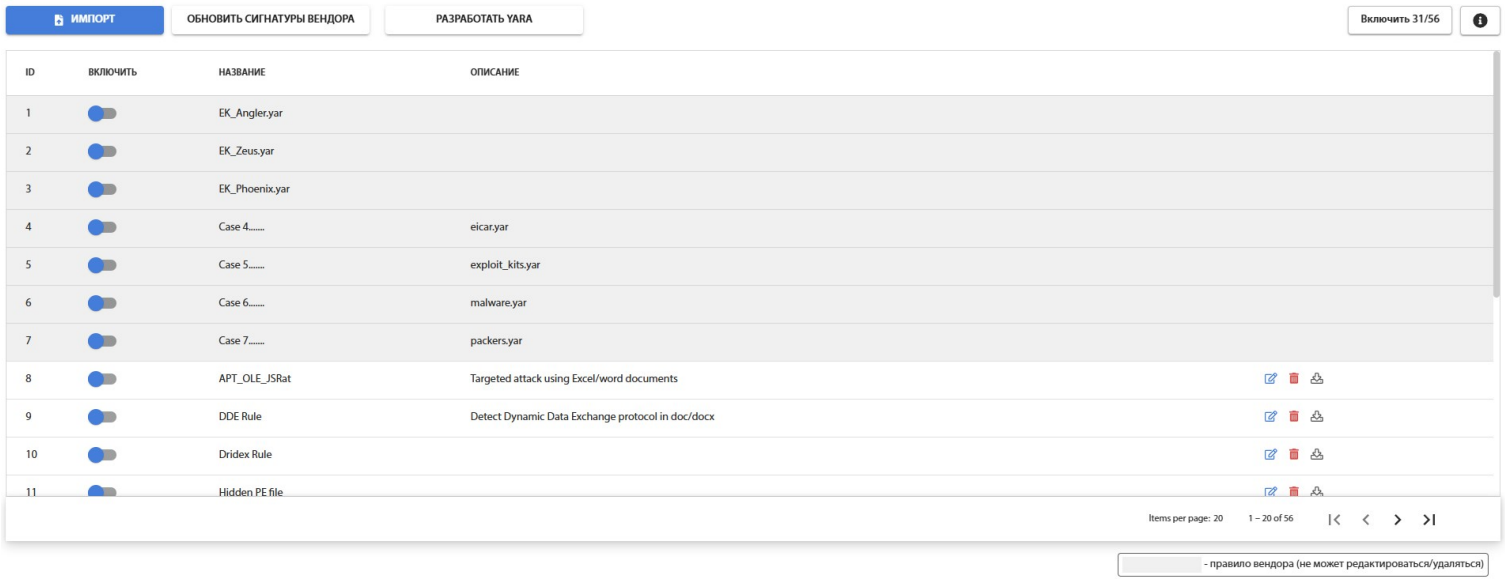


Рис. 4.6.1 - таблица yara-сигнатур

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

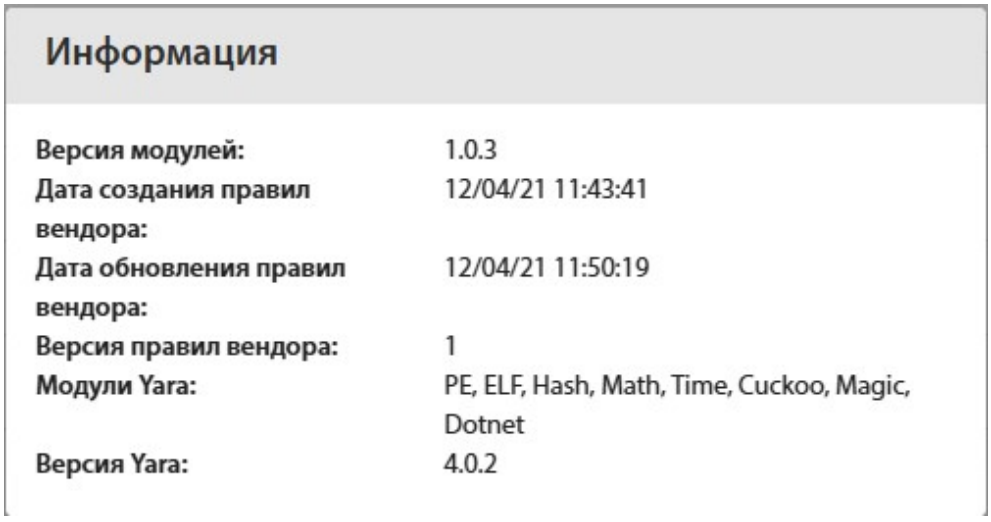


Рис. 4.6.2 - окно с подробной информацией о Yara

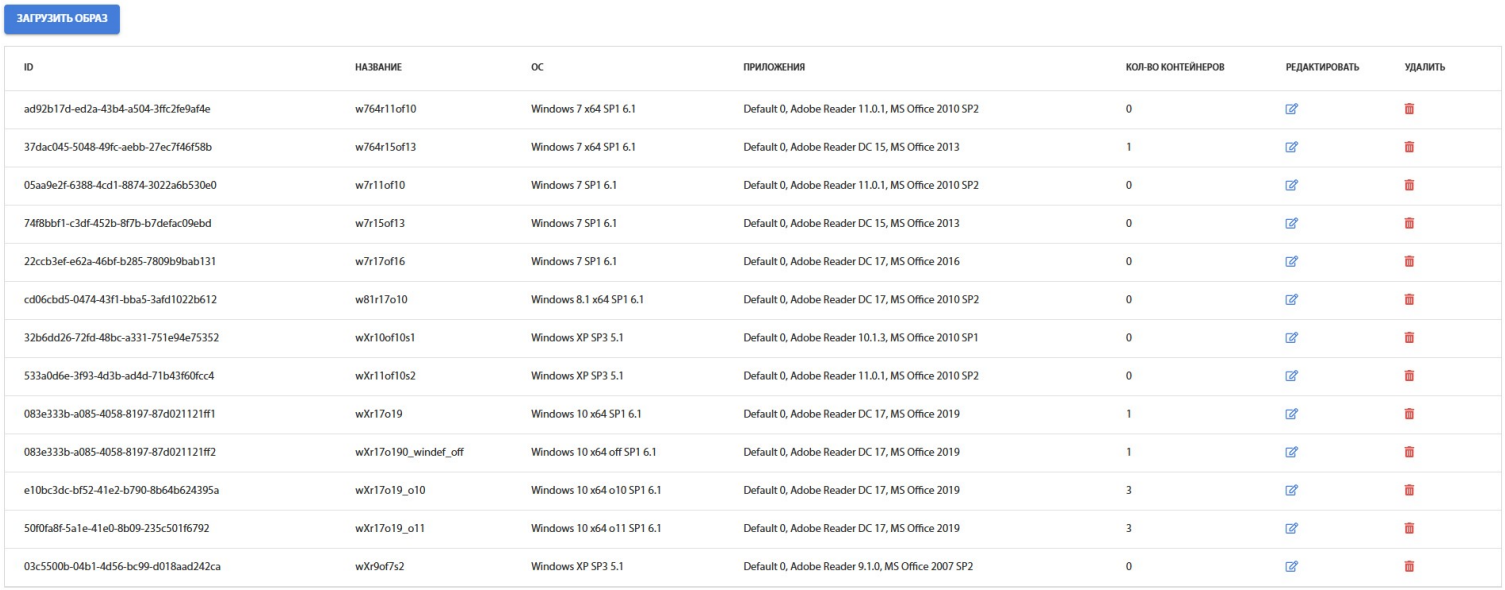
Кнопка ⬇ позволяет скачать Yara-сигнатру файлом формата .yara.

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.

Управление контейнерами

Страница, на которой отображается список контейнеров в системе. Добавленные в таблице контейнеры, доступны для анализа и их статус отображается в Управление - Статус системы.



ID	НАЗВАНИЕ	ОС	ПРИЛОЖЕНИЯ	КОЛ-ВО КОНТЕЙНЕРОВ	РЕДАКТИРОВАТЬ	УДАЛИТЬ
ad92b17d-ed2a-43b4-a504-3ffc2fe9af4e	w764r11of10	Windows 7 x64 SP1 6.1	Default 0, Adobe Reader 11.0.1, MS Office 2010 SP2	0		
37dac045-5048-49fc-aebb-27ec7f46f58b	w764r15of13	Windows 7 x64 SP1 6.1	Default 0, Adobe Reader DC 15, MS Office 2013	1		
05aa9e2f-6388-4cd1-8874-3022a6b530e0	w7r11of10	Windows 7 SP1 6.1	Default 0, Adobe Reader 11.0.1, MS Office 2010 SP2	0		
74f8bbf1-c3df-452b-8f7b-b7defac09ebd	w7r15of13	Windows 7 SP1 6.1	Default 0, Adobe Reader DC 15, MS Office 2013	0		
22ccb3ef-e62a-46bf-b285-7809b9bab131	w7r17of16	Windows 7 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2016	0		
cd06cbd5-0474-43f1-bba5-3afd1022b612	w81r17o10	Windows 8.1 x64 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2010 SP2	0		
32b6dd26-72fd-48bc-a331-751e94e75352	wXr10of10s1	Windows XP SP3 5.1	Default 0, Adobe Reader 10.1.3, MS Office 2010 SP1	0		
533a0d6e-3f93-4d3b-ad4d-71b43f60fcc4	wXr11of10s2	Windows XP SP3 5.1	Default 0, Adobe Reader 11.0.1, MS Office 2010 SP2	0		
083e333b-a085-4058-8197-87d021121ff1	wXr17o19	Windows 10 x64 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2019	1		
083e333b-a085-4058-8197-87d021121ff2	wXr17o190_windef_off	Windows 10 x64 off SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2019	1		
e10bc3dc-bf52-41e2-b790-8b64b624395a	wXr17o19_o10	Windows 10 x64 o10 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2019	3		
50f0fa8f-5a1e-41e0-8b09-235c501f6792	wXr17o19_o11	Windows 10 x64 o11 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2019	3		
03c5500b-04b1-4d56-bc99-d018aad242ca	wXr9of7s2	Windows XP SP3 5.1	Default 0, Adobe Reader 9.1.0, MS Office 2007 SP2	0		

Рис. 4.7.1. - таблица контейнеров

Для того, чтобы добавить новый контейнер, необходимо нажать на кнопку **ЗАГРУЗИТЬ ОБРАЗ**. Доступно два вида импорта:

1. Импорт через локальный путь
2. Импорт через URL

Интеграция

В рамках интеграции представлен функционал по интеграции системы с различными внешними сервисами и ресурсами, которые помогают улучшить ее функциональность и эффективность. Здесь доступны различные настройки и подробная информация. Доступен данный функционал в Управление - Интеграция.

Представлены следующие секции: сетевое хранилище, интеграция Trend micro, ICAP сервер.

Сетевое хранилище

Страница, на которой отображается список сетевых хранилищ (общих папок / shares).В таблице представлены следующие характеристики хранилищ:

1. Включено / выключено сканирование по расписанию
2. Название
3. Сервер (IP)
4. Путь
5. Расписание сканирования (настраивается)
6. Тип сканирования: полное и быстрое. Быстрое - пропускает просканированные файлы по расписанию за период, установленный в поле "Дни до истечения".
7. Имя предустановки

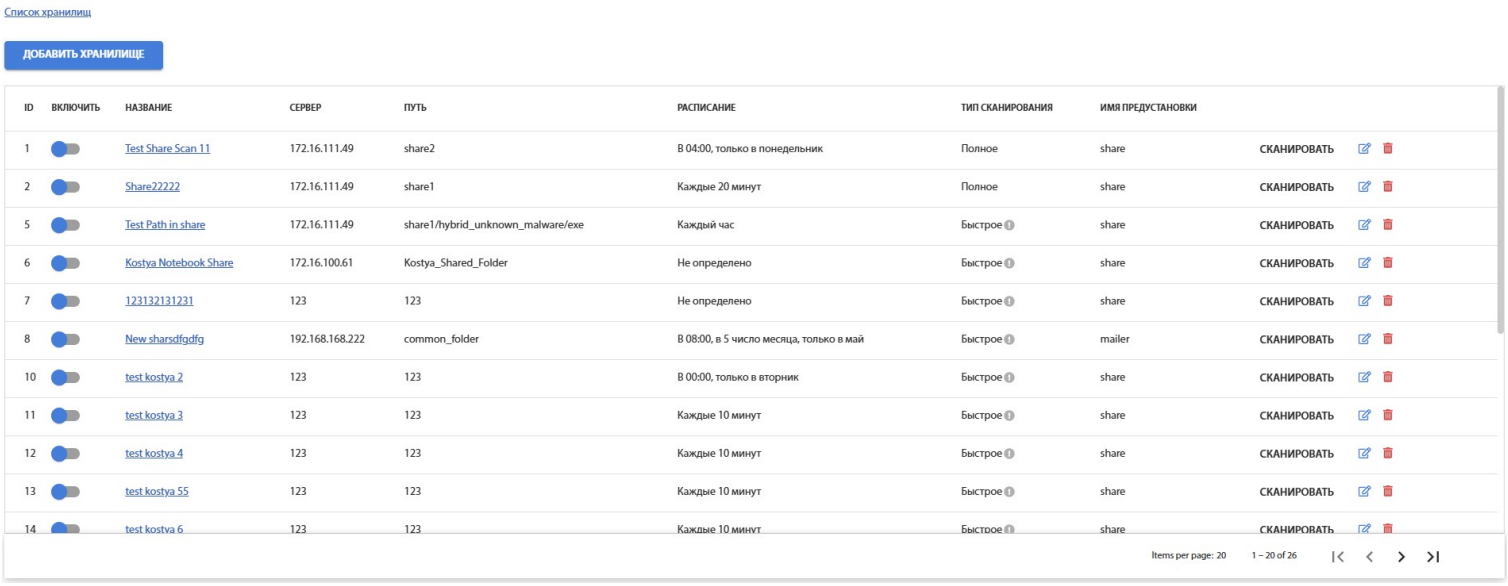


Рис. 4.8.1 - таблица сетевых хранилищ

Для просмотра сессий сканирования определенного хранилища, нужно нажать наназвание хранилища.

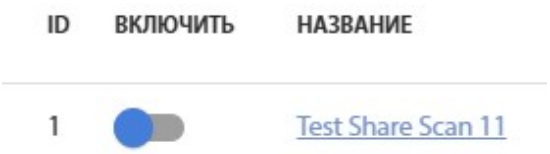


Рис. 4.8.2 - ссылка на сканирования

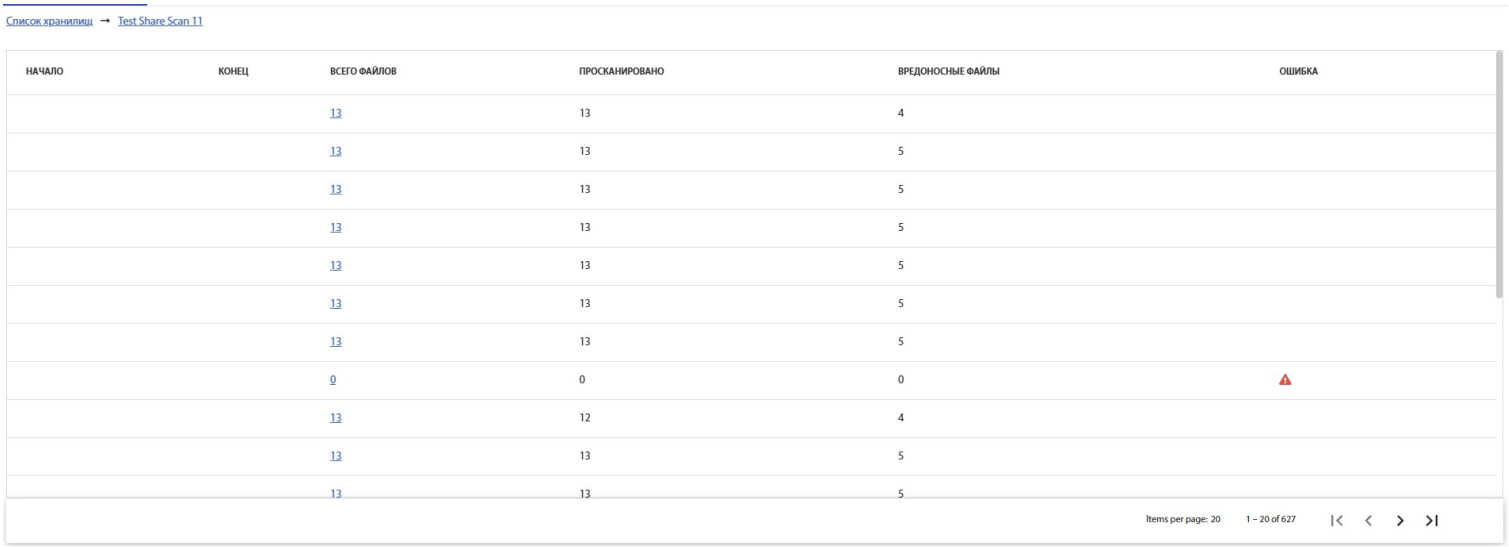


Рис. 4.8.3 - таблица сессий сканирования хранилища

При сканировании хранилища существует вероятность ошибки при выполнении. В случае, если произошла ошибка, в столбце "Ошибка" будет присутствовать знак ⚠. При нажатии на него, появится описание ошибки.

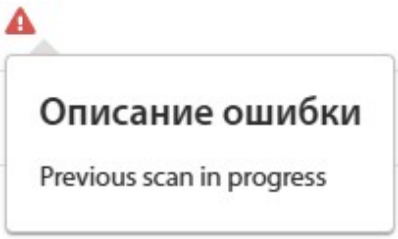


Рис. 4.8.4 - описание ошибки при сканировании

Рис. 4.8.4.1 - навигация на странице сетевые хранилища

Навигация по странице производится нажатием на ссылки на рисунке 4.8.4.1

Для просмотра списка файлов, которые были проанализированы в рамках сканирования, нужно нажать на ссылку, которая активируется при нажатии на числовоезначение в столбце "Всего файлов".

Рис. 4.8.5 - ссылка на таблицу проанализированных файлов

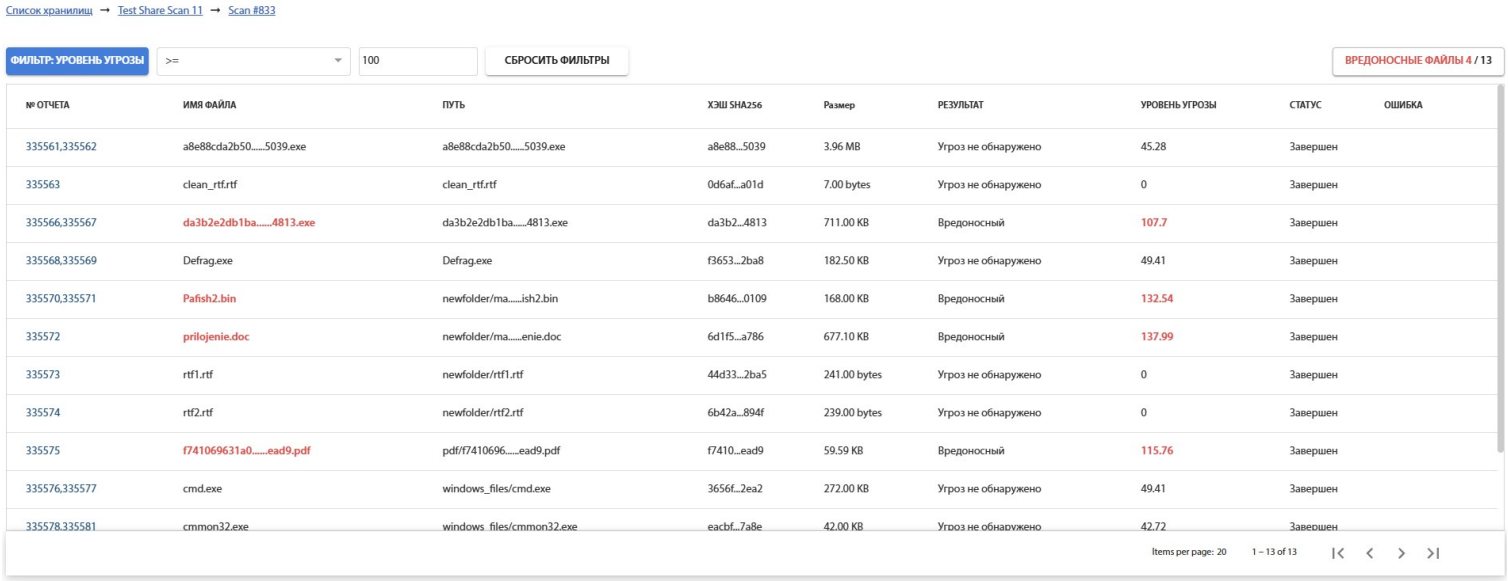


Рис. 4.8.6 - таблица проанализированных файлов

Переход на отчёт анализа файла производится путём нажатия на номер отчёта в столбце "№ Отчета".

ICAP сервер

Страница, на которой осуществляются настройки ICAP сервера и настройки фильтра.

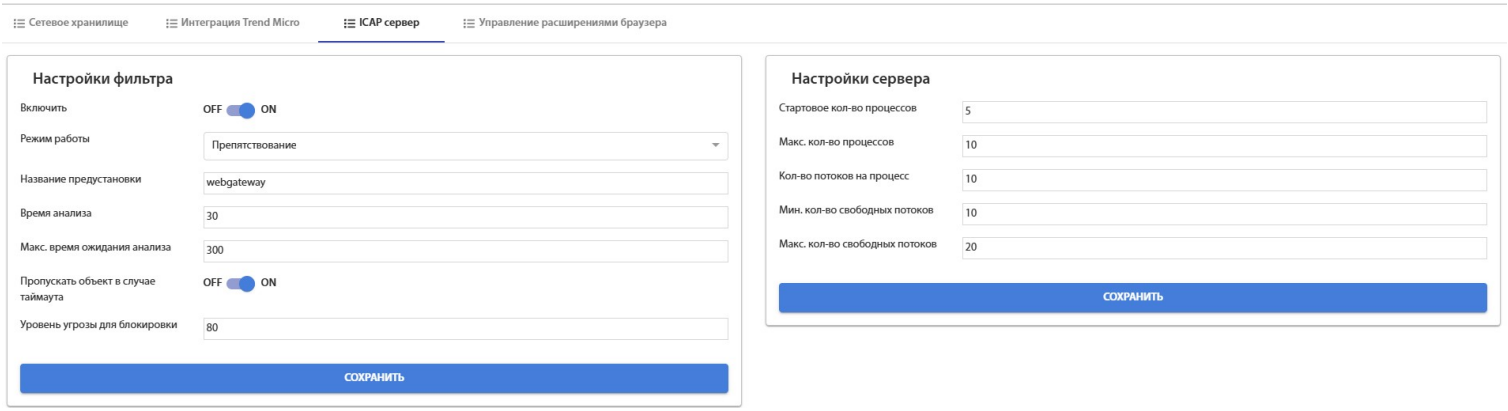


Рис. 4.9.1 - страница настроек ICAP

Корзина

Удаленные администратором отчеты помещаются в корзину. Отсюда их можно восстановить, либо очистить корзину. Отчеты в корзине можно просматривать попрямой ссылке или из корзины.

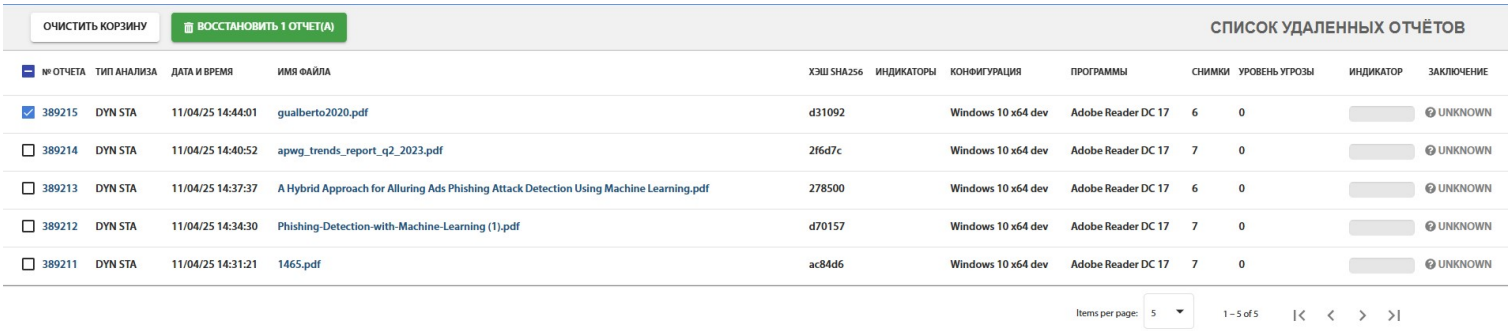


Рис. 5 - Страница корзины отчётов