УТВЕРЖДЕН
НПЕШ.00404-01 90-ЛУ

СИСТЕМА АНАЛИЗА СЕТЕВОГО ТРАФИКА ДЛЯ ОБНАРУЖЕНИЯ КИБЕРАТАК ESENSOR»

Руководство пользователя

НПЕШ.00404-01 90

Листов 102

2025

АННОТАЦИЯ

Настоящий документ представляет собой руководство пользователя изделия «Система анализа сетевого трафика для обнаружения кибератак eSensor» НПЕШ.00404-01 (далее – eSensor, изделие).

В документе содержатся следующие сведения:

– назначение программы (п. 1 настоящего документа);

– условия выполнения программы (п. 2 и 3 настоящего документа);

– описание функций и особенностей эксплуатации изделия (п. 4 настоящего документа).

Настоящий документ предназначен для пользователей и администраторов eSensor.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

BPF	—	(англ. *Berkley Packet Filter*) – технология фильтрации пакетов
FTP	—	(англ. *File Transfer Protocol*) – протокол передачи файлов
ID	—	(англ. *Identification Data*) - идентификатор
SIEM	—	(англ. *Security information and event management*) – управление информацией о безопасности и событиями безопасности
SMB	—	(англ. *Server Message Block*) – сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
TCP	—	(англ. *Transmission Control Protocol*) – один из основных протоколов передачи данных интернета, предназначенный для управления передачей данных
UDP	—	(англ. *User Datagram Protocol*) – протокол пользовательских датаграмм) – один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета
URL	—	(англ. *Uniform Resource Locator*) – унифицированный указатель ресурса
АРМ	—	автоматизированное рабочее место
ИБ	—	информационная безопасность
ПО	—	программное обеспечение
ОС	—	операционная система
eSensor	—	система анализа сетевого трафика для обнаружения кибератак eSensor
СУС	—	сервер управления сенсорами

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Общая информация

eSensor предназначен для обнаружения компьютерных атак на оборудование сетей связи и передачи данных, подключенные к ним комплексы средств автоматизации и автоматизированные (информационные) системы управления.

Изделие обеспечивает анализ сетевого трафика, проходящего через оборудование средств связи, с использованием сигнатурных и эвристических методов с последующей регистрацией событий ИБ. Анализ сетевого трафика происходит с помощью сенсоров. Сенсоры устанавливаются на те узлы исследуемой сети, через которые проходит интересующий с точки зрения информационной безопасности сетевой трафик.

Изделие обеспечивает управление сенсорами, входящими в состав eSensor. Сенсор представляет собой специальный компонент eSensor, который обеспечивает анализ сетевого трафика, проходящего через узел исследуемой сети, на котором установлено данное программное обеспечение (далее – ПО). При обнаружении событий информационной безопасности (далее – ИБ) сенсоры сохраняют эту информацию в базе данных.

Изделие обеспечивает управление встроенной базой решающих правил сигнатурного анализа.

Изделие обеспечивает захват сетевого трафика, проходящего через оборудование средств связи, с последующей записью данного трафика в PCAP-файлы.

Изделие обеспечивает управление PCAP-файлами, а именно:

– экспорт записанных PCAP-файлов из eSensor;

– импорт файлов в eSensor;

– проверку импортированных или созданных в процессе работы eSensor PCAP-файлов модулями изделия с использованием сигнатурных и эвристических методов.

Изделие обеспечивает анализ фрагментированного сетевого трафика.

Изделие обеспечивает передачу обнаруживаемых событий ИБ в SIEM-системы.

В случае недоступности по каким-либо причинам подключения к SIEM-системе, изделие обеспечивает накопление информации обо всех событиях ИБ, выявленных в автономном режиме и последующую передачу этой информации в SIEM-систему при восстановлении подключения.

Изделие выявляет событие ИБ на оборудовании сетей связи в режиме реального времени. Для выявления событий ИБ eSensor производит непрерывный мониторинг сетевого трафика, проходящего через оборудование средств связи.

1.2. Основной алгоритм работы

Основной алгоритм работы eSensor состоит из следующих этапов:

1) сенсоры eSensor захватывают поступающий на них сетевой трафик;

2) сенсоры разбирают трафик по протоколам и регистрируют информацию о сетевых взаимодействиях – сессиях;

Примечание. Сенсоры умеют регистрировать сессии, проходящие с использованием следующих протоколов: IPv4, IPv6, IP in IP, ICMPv4, ICMPv6, TCP, UDP, IPSEC (ESP, AH), GRE, OSPF, SCTP.

3) сенсоры анализируют трафик на наличие в нем вредоносной активности с использованием сигнатурных и эвристических методов. Сигнатурный анализ – это анализ заголовков протоколов и содержимого сетевых пакетов на соответствие заранее определенным сигнатурам с использованием так называемых решающих правил. При эвристическом анализе выявляется наличие аномального поведения в сетевом трафике с использованием различных эвристик. Данный вид анализа применяется, когда для выявления атаки невозможно использовать какую-либо сигнатуру;

4) сенсоры записывают сетевой трафик и сохраняют его. Записанный трафик можно отправить на повторную проверку. Это может быть полезно, например, для обнаружения в трафике новых атак, если обновилась база решающих правил. Помимо этого, хранящийся трафик можно экспортировать в формате PCAP;

5) сенсор может отправлять информацию о регистрируемых им событиях ИБ в SIEM-систему.

eSensor поддерживает решающие правила, синтаксис которых соответствует Suricata 5. Описание возможностей по управлению правилами приведено в разделе 4.6.5 настоящего документа.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования к среде функционирования

Перед эксплуатацией изделия необходимо внимательно ознакомиться с эксплуатационной документацией, входящей в состав поставки eSensor.

Для ПО среды функционирования eSensor должны быть установлены все актуальные обновления, выпущенные предприятием-изготовителем, а также выполнены рекомендации предприятия-изготовителя по безопасному конфигурированию.

При эксплуатации изделия на объектах информатизации, где производится обработка конфиденциальной информации, необходимо выполнение следующих условий:

– наличие администратора безопасности, отвечающего за правильную эксплуатацию (включая рекомендации по безопасному конфигурированию комплекса) eSensor;

– обеспечение физической сохранности рабочей станции с установленным eSensor и исключение возможности доступа к ней/ним посторонних лиц;

– проведение периодического контроля целостности, установленного eSensor с помощью программ контроля целостности (не реже одного раза в месяц);

– периодическое обновление базы решающих правил в eSensor;

– проведение периодической проверки eSensor и среды его функционирования на наличие компьютерных вирусов с использованием средств антивирусной защиты (не реже одного раза в месяц);

– наличие организационных и технических мер, направленных на исключение несанкционированного доступа к объекту функционирования eSensor.

Для защиты каналов передачи данных eSensor, в том числе выходящих за пределы контролируемой зоны, должны применяться сертифицированные в установленном порядке методы и средства, устойчивые к пассивному и/или активному прослушиванию сети, или должен быть запрещен удаленный доступ для администрирования eSensor по незащищенным каналам связи.

При эксплуатации eSensor оператором информационной системы должно быть обеспечено выполнение всех необходимых усилений мер защиты информации.

2.2. Установка и условия выполнения eSensor

Установка и первичная настройка eSensor осуществляется администратором в соответствии с документом «Система анализа сетевого трафика для обнаружения кибератак eSensor. Руководство администратора» НПЕШ.00404-01 91.

Условия выполнения eSensor на автоматизированном рабочем месте (далее – АРМ) указаны в документе «Система анализа сетевого трафика для обнаружения кибератак eSensor. Руководство администратора» НПЕШ.00404-01 91.

Примечание. Любые действия, непосредственно проводимые с АРМ, необходимо осуществлять в соответствии с документацией на этот АРМ.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Подготовка к запуску eSensor

Для подготовки к запуску eSensor необходимо выполнить следующие действия:

– получить АРМ с установленным на него eSensor с комплектом документации;

– запустить АРМ в соответствии с эксплуатационной документацией на него (eSensor будет запущен автоматически);

– подключиться к веб-интерфейсу eSensor в соответствии с п. 3.2 настоящего документа.

3.2. Запуск eSensor

Для подключения к веб-интерфейсу eSensor необходимо выполнить следующие действия:

– включить АРМ в соответствии с эксплуатационной документацией на него;

– открыть браузер и в адресной строке ввести: https://<Адрес_СУС>:7100/, где <Адрес_СУС> – адрес, по которому доступен сервер управления сенсорами (далее – СУС);

– перейти по введенной ссылке;

– далее в окне браузера отобразится окно авторизации eSensor (рис. 1).

4. ВЕБ-ИНТЕРФЕЙС ESENSOR

4.1. Общее описание веб-интерфейса eSensor

После подключения к eSensor в браузере отобразится окно авторизации, где пользователь должен ввести логин и пароль (рис. 1).

Для получения логина и пароля для авторизации в eSensor обратитесь к своему администратору (пользователю с ролью «Администратор»).

Окно авторизации

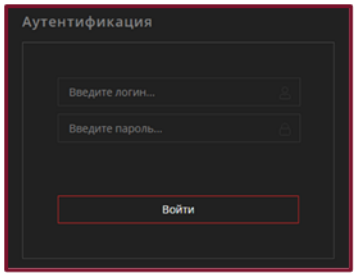

Рис. 1

При успешной авторизации в веб-интерфейсе будет отображена главная страница eSensor (рис. 2).

Главная страница eSensor

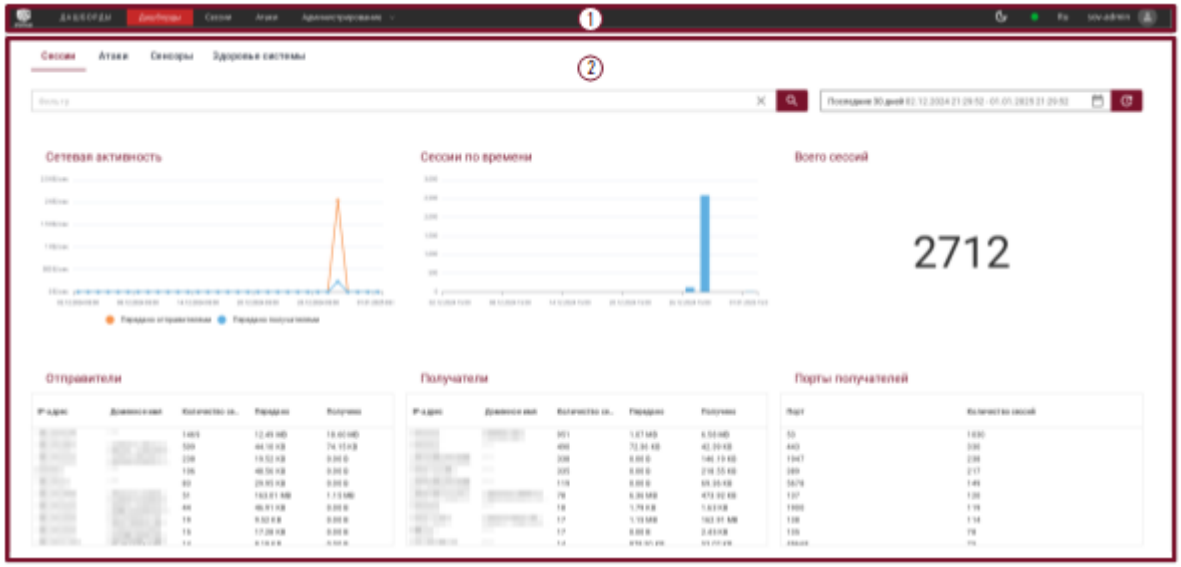

Рис. 2

Веб-интерфейс eSensor содержит два основных блока элементов:

– «Панель навигации» (см. № 1 на рис. 2);

– «Рабочее окно» (см. № 2 на рис. 2).

Блок «Панель навигации» всегда отображается в верхней части интерфейса eSensor и используется для быстрого доступа к функциям изделия и навигации. Быстрый переход к функциям eSensor обеспечивают следующие разделы и элементы:

– раздел «Дашборды» (п. 4.3 настоящего документа);

– раздел «Сессии» (п. 4.4 настоящего документа);

– раздел «Атаки» (п. 4.5 настоящего документа);

– выпадающее меню «Администрирование» (п. 4.6 настоящего документа);

– меню выбора темы оформления интерфейса (иконка « » на рис. 2);

– индикатор общего состояния компонентов eSensor (иконка « » на рис. 2);

– меню выбора языка интерфейса (иконка « Ru » или «En» на рис. 2);

– имя текущего пользователя (пример на рис. 2 – «sov-admin»);

– меню управления учетной записью пользователя (иконка « » на рис. 2 и п. 4.2 настоящего документа).

Блок «Рабочее окно» является основной рабочей областью интерфейса eSensor, в котором отображается информация о работающих сенсорах изделия.

Веб-интерфейс изделия поддерживает унифицированный механизм отображения данных в табличном формате, при этом пользователю предоставляется возможность управлять данными этих таблиц.

4.1.1. Иконки, используемые в графическом интерфейсе

В таблице 1 представлено назначение стандартных иконок, используемых в графическом интерфейсе eSensor.

Таблица 1 – Используемые иконки и их назначение

Иконка	Назначение
	Кнопка перехода на главную страницу
	Меню выбора темы оформления интерфейса
   	Индикатор общего состояния компонентов в блоке «Панель навигации». При нажатии в навигационном меню открывает информационную панель «Последние проблемы», появляющуюся в правой части рабочего окна (позволяет перейти к дашборду здоровья системы). Возможные состояния и значения индикатора: – «  » – сигнализирует об отсутствии каких-либо проблем с функционированием компонентов изделия на данный момент времени; – «  » – сигнализирует о том, что в процессе функционирования были зафиксированы некоторые проблемы; – «  » – сигнализирует о серьезных проблемах в функционировании компонентов изделия; – «  » – сигнализирует об отсутствии данных о состоянии компонентов
Ru / En	Меню выбора языка интерфейса
	Меню управления учетной записью пользователя
	Кнопка «Удалить»
	Кнопка «Закрыть» / «Отменить»
	Кнопка «Добавить»
	Свернуть выпадающий список
	Развернуть выпадающий список
	Перейти к предыдущей странице
	Перейти к следующей странице
	Кнопка «Поиск»
	Кнопка «Обновить время»
	Кнопка «Выбрать время»
	Кнопка «Фильтр по времени»
	Кнопка «Настройка отображения столбцов таблицы»
	Сообщение об ошибке
	Кнопка «Обновить правила сенсора». Отображается только для сенсоров, на которых необходимо обновить правила, при этом у сенсора должен быть статус подключения «  » (подключен)

Иконка	Назначение
	Кнопка «Уменьшить ширину строк таблицы»
	Кнопка «Увеличить ширину строк таблицы»
	Кнопка «Сортировка по возрастанию»
	Кнопка «Сортировка по убыванию»
	Кнопка «Импортировать»
    	Индикатор общего состояния подключения СУС к сенсору. Данный индикатор используется на вкладках со статусами подключения сенсоров: – «Дашборды» → «Сенсоры»; – «Администрирование» → «Сенсоры». Для отображения общего состояния подключения СУС к выбранному сенсору используются следующие иконки: – «  » – означающий статус «Подключен»; – «  » – означающий статус «Добавлен»; – «  » – означающий статус «Закрыт»; – «  » – означающий статус «Сбой связи»; – «  » – означающий статус «Не определен»
   	Индикатор уровня опасности атак, обнаруженных изделием. Используется в карточках и виджетах атак, а также в карточке сессии на графике атак и т.д. Данный индикатор может использоваться в изделии без указания цифр внутри, но имеет аналогичные значения в соответствии с представленными цветами. Возможные состояния и значения индикатора: – «  » – сигнализирует о критическом уровне опасности атаки; – «  » – сигнализирует о высоком уровне опасности атаки; – «  » – сигнализирует о среднем уровне опасности атаки; – «  » – сигнализирует о низком уровне опасности атаки
	Индикатор предупреждения в случае, когда сенсором со статусом подключения «  » используется не последняя версия группы правил. Подсказка активируется наведением курсора на иконку. Данный индикатор используется на следующих вкладках: – «Дашборды» → «Сенсоры»; – «Администрирование» → «Сенсоры»; – «Группы правил» → «Группа» → «Сенсоры»; – «Администрирование» → «Сенсоры» → «Сенсор» → *любой модуль сенсора*

Иконка	Назначение
	Кнопка «Создать запрос на копирование дампов». Становится доступна при выборе одной или нескольких сессий путем активации чекбоксов в необходимых строках в информационной таблице «Сессии». Используется также в информационной таблице «Сессии» как индикатор того, что на выбранной сессии дамп был скопирован в хранилище

Информационная панель «Последние проблемы» представлена на рис. 3.

Информационная панель «Последние проблемы»

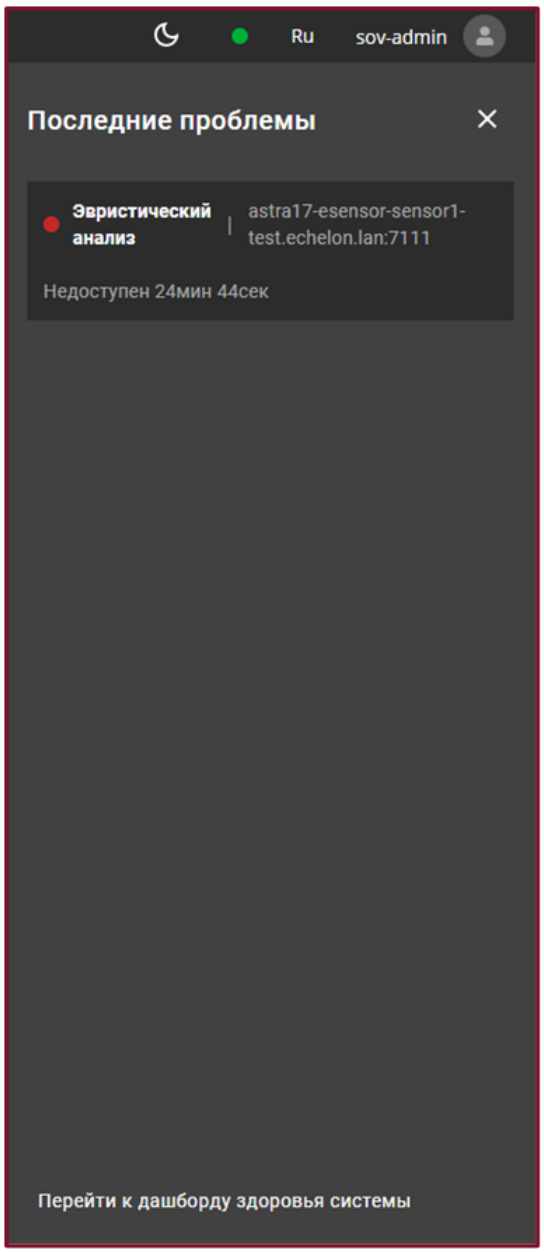

Рис. 3

4.1.2. Настройка отображения столбцов таблицы и сортировка данных

Иконка настройки отображения столбцов таблицы «⚙» предназначена для выбора отображения необходимых пользователю столбцов, доступных в зависимости от текущей таблицы (пример см. на рис. 4).

Настройка отображения столбцов таблицы на вкладке «Сессии»

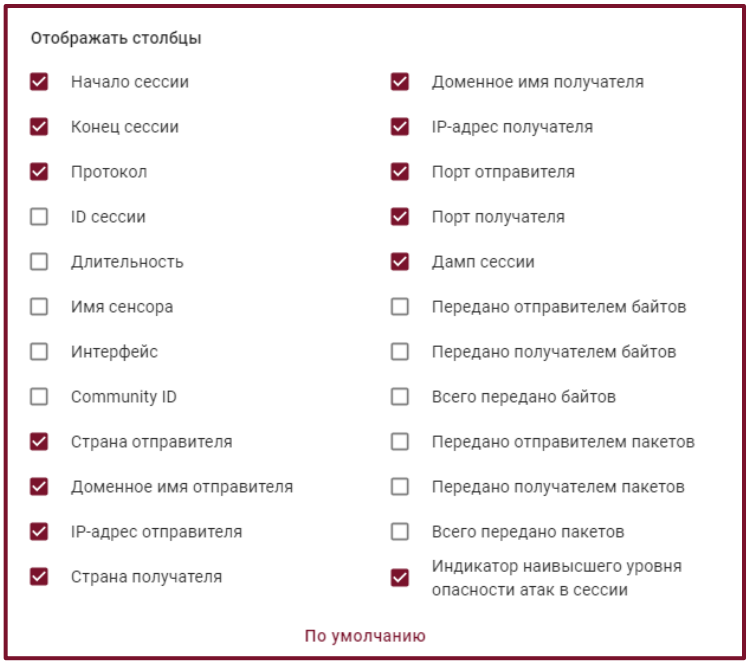

Рис. 4

Выбрать/убрать отображение столбца можно нажатием на его название или поле выбора «☐» рядом с его названием. После чего выбранный столбец отобразится в таблице, а в настройках отображения появится «☑» рядом с добавленным столбцом. Такой чекбокс считается активированным.

В таблицах eSensor предусмотрена сортировка строк таблицы по необходимому столбцу для упрощения поиска интересующей информации.

Для использования доступен вид сортировки: «↑» (по возрастанию) и «↓» (по убыванию). Иконки «↑» и «↓» становятся доступны при наведении курсором на интересующий столбец, переключаются дополнительным нажатием и остаются видны (активны) рядом с наименованием выбранного столбца.

Отменить все дополнительные настройки отображения таблиц и активной сортировки можно нажав кнопки «⚙» → «По умолчанию».

4.1.3. Фильтрация по специальным выражениям

Для удобства обработки информации в eSensor предусмотрена фильтрация информации (о сессиях, атаках) с использованием специальных выражений с помощью поля «Фильтрация» (рис. 5).

Поле «Фильтрация»

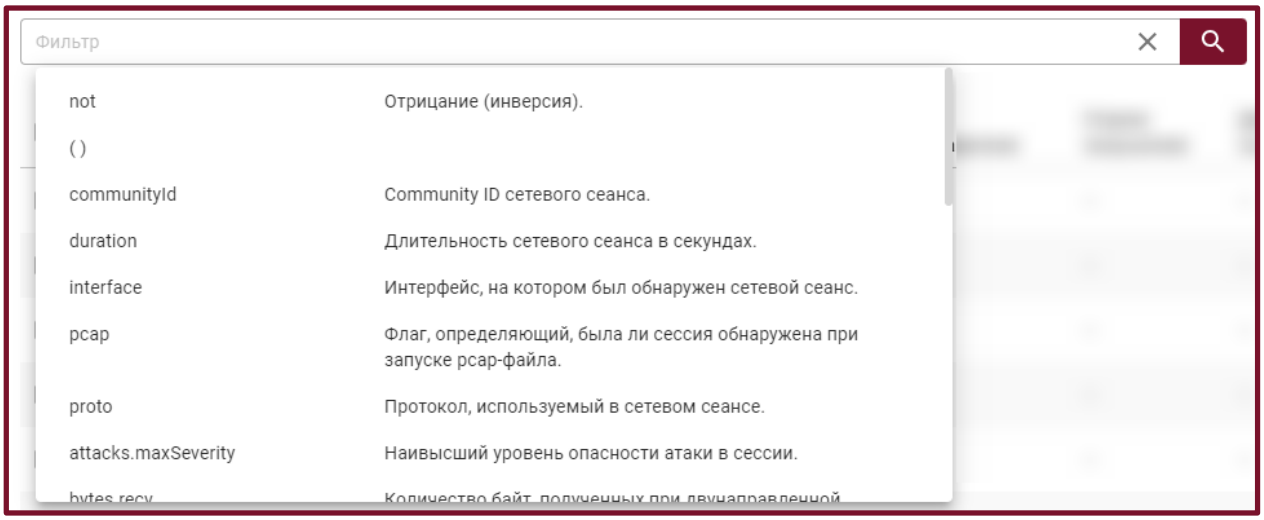

Рис. 5

Для применения фильтрации информации необходимо составить и задать специальное выражение фильтрации, используя, например, один из следующих атрибутов:

– `not` – отрицание (инверсия);

– `( )` – скобки используются для выделения каких-либо выражений и применения к ним оператора. Например, `not (proto == tcp and dst.port == 9000)`. Этот фильтр позволяет получить только те сессии, в которых протокол — не TCP, и при этом порт получателя — не 9000;

– `proto` – протокол транспортного уровня, использованный в сессии/атаке;

– `bytes.recv` – количество байт, переданных получателем сессии;

– `bytes.sent` – количество байт, переданных отправителем сессии;

– `bytes.total` – общее количество байт, переданных в рамках сессии;

– `dst.ip` – IP-адрес получателя;

– `dst.port` – порт получателя;

– `pkts.recv` – количество пакетов, переданных получателем сессии;

– `pkts.sent` – количество байт, переданных отправителем сессии;

– `pkts.total` – общее количество пакетов, переданных в рамках сессии;

– `sensor.name` – имя сенсора, зарегистрировавшего сессию/обнаружившего атаку;

– `src.ip` – IP-адрес отправителя;

– `src.port` – порт отправителя.

После выбора нужного атрибута необходимо нажать пробел, после чего откроется список операторов сравнения. Примеры операторов:

– `<` – проверяет, что значение меньше следующего;

– `>` – проверяет, что значение больше следующего;

– `<=` – проверяет, что значение меньше или равно следующему;

– `>=` – проверяет, что значение больше или равно следующему;

– `= =` – проверяет, что значения равны;

– `!=` – проверяет, что значения не равны;

– `in` – проверяет, что элемент представлен в списке;

– `~` – проверяет, что строка соответствует паттерну, с учетом регистра. Паттерн может содержать символы;

– `!~` – проверяет, что строка не соответствует паттерну, с учетом регистра. Паттерн может содержать символы;

– `~*` – проверяет, что строка соответствует паттерну, без учета регистра. Паттерн может содержать символы;

– `!~*` – проверяет, что строка не соответствует паттерну, без учета регистра. Паттерн может содержать символы.

Примечание. В списках атрибутов и операторов приведены только некоторые из доступных пользователю. С полным списком можно ознакомиться в выпадающей динамической подсказке под полем «Фильтрация».

После ввода специального выражения фильтрации для активации фильтрации по заданному параметру необходимо нажать «🔍».

Если специальное выражение фильтрации задано с ошибкой или некорректно, то поле «Фильтрация» будет выделено красным и появится иконка «ⓘ», при наведении на которую можно будет увидеть сообщение об ошибке (рис. 6).

Сообщение об ошибке поля «Фильтрация»

Рис. 6

При активации фильтрации с помощью поля «Фильтрация» **используемый фильтр дополнительно применится к аналогичному разделу изделия**, например:

– использование фильтрации по специальным выражениям на вкладке «Сессии» раздела «Дашборды» также автоматически применится к разделу «Сессии»;

– использование фильтрации по специальным выражениям на вкладке «Атаки» раздела «Дашборды» также автоматически применится к разделу «Атаки».

4.1.4. Фильтрация по времени

Для удобства обработки информации в eSensor предусмотрена фильтрация информации по указанному пользователем периодом времени. Чтобы настроить отображение информации за указанный период времени необходимо нажать на поле с иконкой «» после чего отобразится окно настроек «Фильтрация по времени» (см. рис. 7).

Окно настроек «Фильтрация по времени»

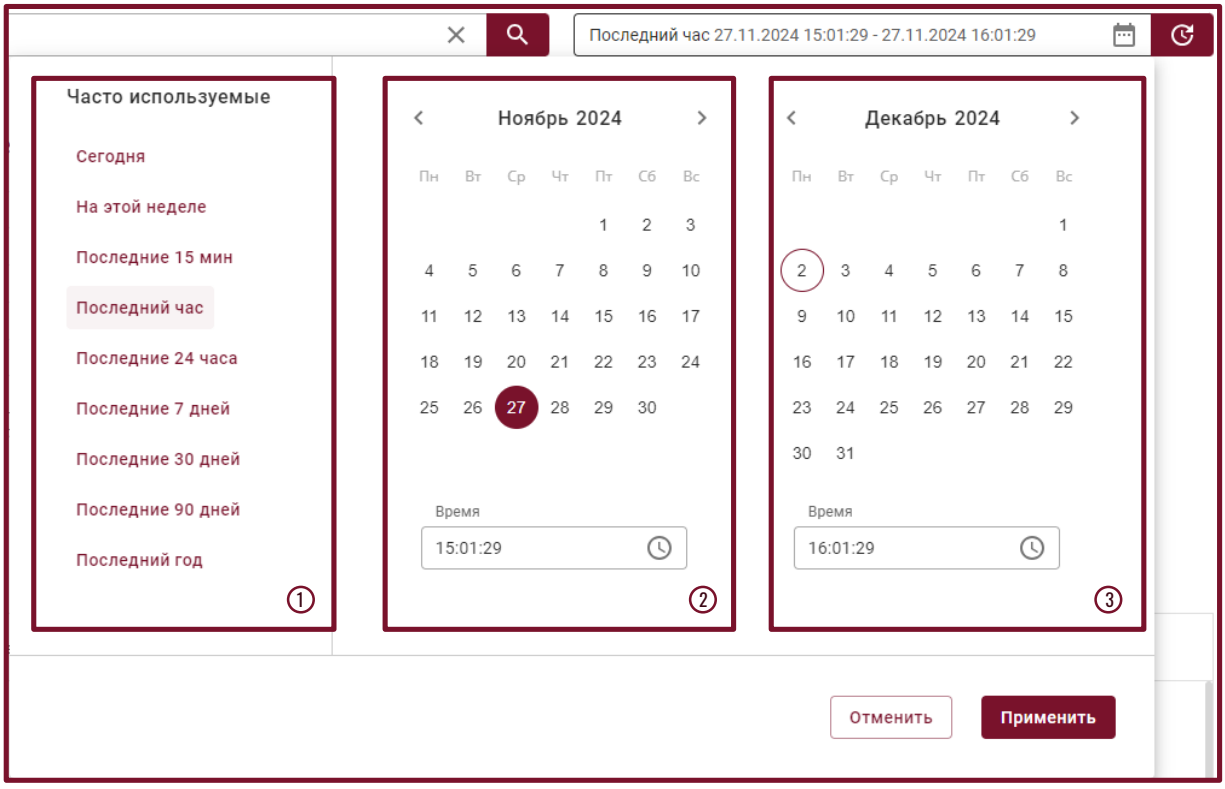

Рис. 7

В блоке «Часто используемые» (см. № 1 на рис. 7) левой части окна предусмотрена быстрая настройка отображения информации за определенный промежуток времени – часто используемые фильтры. Нажатием на один из вариантов, представленных в данной части окна настроек, можно установить один из следующих вариантов отображения информации:

– «Сегодня» – отобразится информация, зарегистрированная за текущую дату;

– «На этой неделе» – отобразится информация, зарегистрированная за текущую неделю;

– «Последние 15 мин» – отобразится информация, зарегистрированная за прошедшие 15 минут;

– «Последний час» – отобразится информация, зарегистрированная за прошедший час;

– «Последние 24 часа» – отобразится информация, зарегистрированная за прошедшие сутки;

– «Последние 7 дней» – отобразится информация, зарегистрированная за прошедшую неделю;

– «Последние 30 дней» – отобразится информация, зарегистрированная за прошедшие 30 дней;

– «Последние 90 дней» – отобразится информация, зарегистрированная за прошедшие 90 дней;

– «Последний год» – отобразится информация, зарегистрированная за прошедший год.

После нажатия на один из описанных вариантов информация пользователю отобразится только та, которая удовлетворяет установленным фильтрам, а в текстовом поле рядом с иконкой «» отобразится надпись с примененным фильтром.

Блок правой части окна предназначен для настройки отображения информации, зарегистрированной за более точный промежуток времени.

Для установки точного промежутка даты и времени для отображения информации, зарегистрированной за этот промежуток времени, необходимо в первом календаре выбрать дату и время отсчета (см. № 2 на рис. 7), а во втором – дату и время окончания необходимого пользователю временного промежутка (см. № 3 на рис. 7). При этом, в изделии предусмотрена возможность с помощью кнопок «» и поля «Время» выбрать и задать точное время начала и окончания фильтрации информации по времени (рис. 8) с шагом 15 минут.

Настройка поля «Время»

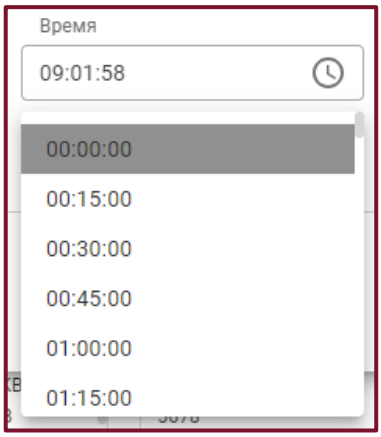

Рис. 8

После настройки параметров отображения информации за определенный промежуток времени необходимо нажать кнопку «Применить» для подтверждения или «Отменить» для отмены внесенных изменений. После чего на странице отобразится только та информация, которая была зарегистрирована сенсорами eSensor за настроенный промежуток времени, а в поле слева от иконки «» отобразится описание примененного фильтра по времени.

ВНИМАНИЕ!

Примененные фильтры из блока «Часто используемые» **не обновляются автоматически** для удобства работы пользователя с отфильтрованной информацией. Чтобы обновить отфильтрованную информацию по примененному ранее фильтру до текущей точки отсчета времени необходимо нажать кнопку «».

4.1.5. Поле «Поиск»

В eSensor на некоторых страницах использующие таблицы (например, выпадающее меню «Администрирование» → раздел «Группы правил» → вкладка «Правила») предусмотрена функция поиска информации по какому-либо заранее известному параметру данных.

Для поиска данных необходимо воспользоваться полем для ввода «Поиск» (рис. 9) и ввести корректный заранее известный параметр поиска данных (например, название правила) нажать на кнопку «🔍» или клавишу «Enter» клавиатуры.

Поле для ввода «Поиск»

Рис. 9

После нажатия кнопки «🔍» eSensor произведет сопоставление введенного параметра всем данным из таблицы и, в случае совпадения параметра данным из таблицы, отобразит только те данные, которые соответствуют условиям поиска. В противном случае в таблице на странице eSensor отобразится сообщение «Нет данных», что сигнализирует об отсутствии совпадений по введенному параметру.

Для возврата к отображению табличных данных по умолчанию (отмены поиска) необходимо нажать на иконку «✕» в строке ввода «Поиск».

4.2. Меню управления учетной записью пользователя

4.2.1.1. Вкладка «О программе»

Для ознакомления с информацией о eSensor предназначен специальный интерфейс, переход к которому осуществляется наведением на иконку «●» на панели навигации, и далее в выпадающем списке нажатием пункта «О программе» (см. рис. 10).

Вкладка «О программе»

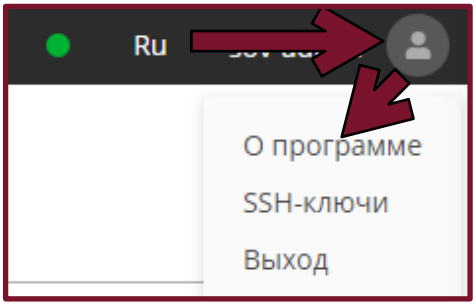

Рис. 10

Окно ознакомления с информацией о продукте представлено на рис. 11.

Окно «О программе»

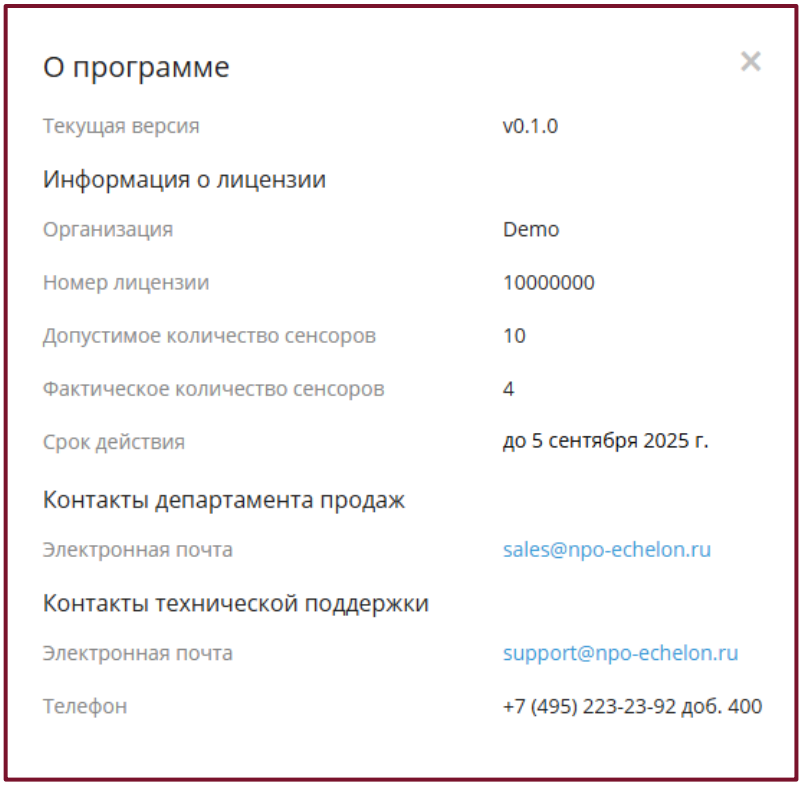

Рис. 11

В окне «О программе» содержатся следующие данные:

1) текущая версия;

2) информация о лицензии:

а) организация;

б) номер лицензии;

в) допустимое количество сенсоров;

г) фактическое количество сенсоров;

д) срок действия.

3) контакты департамента продаж:

а) электронная почта.

4) контакты технической поддержки:

а) электронная почта;

б) телефон.

4.2.1.2. Вкладка «SSH-ключи»

4.2.1.2.1. Общая информация

Для осуществления возможности добавления SSH-ключей пользователя, используемых для скачивания групп правил с СУС на удаленную машину, а также для удаленного разрешения конфликтов, возникающих при работе с группами правил, необходимо навести курсор на иконку « » на панели навигации, и в выпадающем списке нажать пункт «SSH-ключи» (рис. 12).

Вкладка «SSH-ключи»

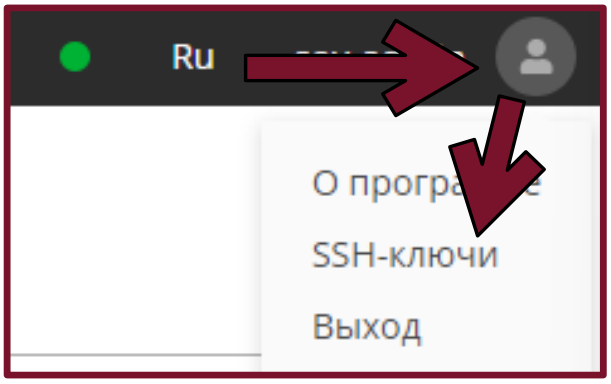

Рис. 12

Далее произойдет переход на страницу «SSH-ключи» (рис. 13), которая позволяет взаимодействовать с ними, а именно:

– просматривать таблицу SSH-ключей пользователя, хранящихся на СУС;

– настраивать таблицу SSH-ключей пользователя, хранящихся на СУС;

– добавлять SSH-ключи пользователя в хранилище СУС (см. п. 4.2.1.2.2 настоящего документа);

– переходить к карточкам SSH-ключей, содержащих подробную информацию о ключах (см. п. 4.2.1.2.3 настоящего документа);

– удалять SSH-ключи пользователя из хранилища СУС (см. п. 4.2.1.2.4 настоящего документа).

Страница «SSH-ключи»

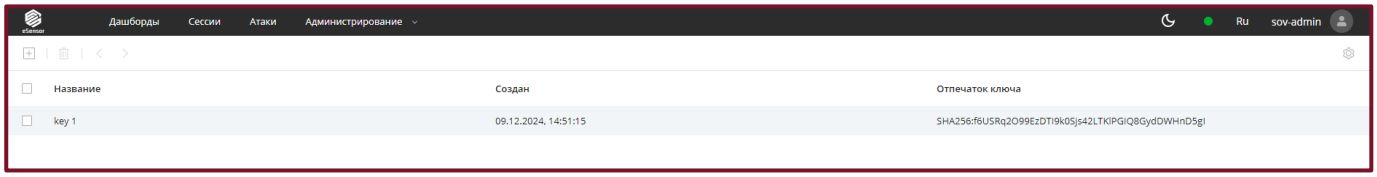

Рис. 13

В рабочей области страницы находится таблица добавленных SSH-ключей пользователя. По умолчанию в таблице отображается следующая информация о каждом SSH-ключе:

– столбец «Название» – отображает наименования SSH-ключей;

– столбец «Создан» – отображает дату и время добавления SSH-ключей;

– столбец «Отпечаток ключа» – отображает криптографический отпечаток, используемый каждой парой SSH-ключей.

4.2.1.2.2. Добавление SSH-ключа пользователя

Для добавления SSH-ключа пользователя в хранилище СУС eSensor необходимо выполнить следующее:

1) авторизоваться в eSensor с учетной записи требуемого пользователя;

2) перейти на страницу «SSH-ключи» и нажать в левой верхней части страницы кнопку «⊞»;

3) на открывшейся странице «Новый SSH-ключ пользователя» (см.рис. 14) заполнить в соответствующих обязательных полях:

а) «Название» – название ключа (пример: rsa 1);

б) «Ключ» – открытый (публичный) SSH-ключ пользователя (пример: ssh-rsa AAaN23ekaLSA1da…). Допустимые типы ключей: RSA любой длины, ECDSA любой длины, ED25519.

Страница «Новый SSH-ключ пользователя»

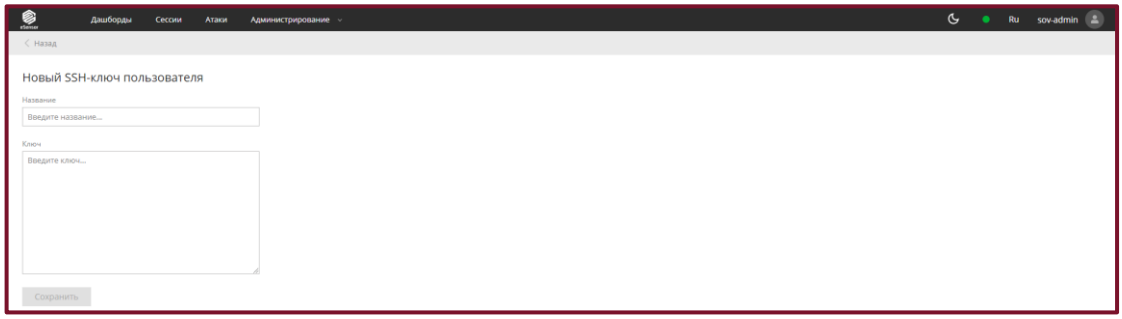

Рис. 14

в) нажать кнопку «Сохранить» для добавления пользовательского SSH-ключа или кнопку «Назад» для отмены и возврата на страницу «SSH-ключи».

4.2.1.2.3. Карточка SSH-ключа пользователя

Для просмотра информации о конкретном пользовательском SSH-ключе необходимо нажать на интересующую строку с ключом в таблице на странице «SSH-ключи». Далее произойдет переход на страницу «Карточка SSH-ключа пользователя» (пример см. на рис. 15).

Страница «Карточка SSH-ключа пользователя»

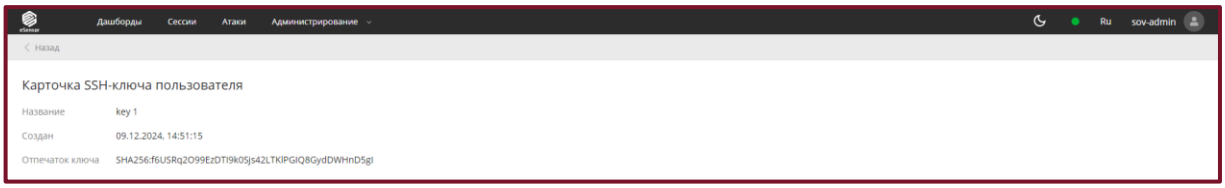

Рис. 15

В карточке отображается следующая информация о SSH-ключе пользователя:

– название, заданное пользователем;

– дата и время создания;

– отпечаток ключа.

4.2.1.2.4. Удаление SSH-ключа пользователя

Для удаления SSH-ключа пользователя из хранилища СУС eSensor необходимо:

1) авторизоваться в eSensor с учетной записи требуемого пользователя;

2) перейти на страницу «SSH-ключи» и выбрать в таблице на странице необходимый SSH-ключ, активировав чекбокс («☑») в строке с информацией о нем;

3) нажать кнопку «🗑» для удаления из eSensor;

4) подтвердить действия, нажав кнопку «Подтвердить» или прервать удаление, нажав кнопку «Отменить» (или «✕») в всплывающем окне «Подтверждение удаления» (рис. 16).

Всплывающее окно «Подтверждение удаления»

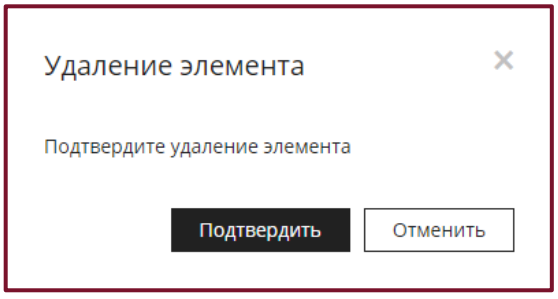

Рис. 16

4.2.1.3. Вкладка «Выход»

Для разрыва текущей сессии пользователя необходимо навести курсор на иконку « » на панели навигации, и далее в выпадающем списке нажать пункт «Выход» (рис. 17).

Вкладка «Выход»

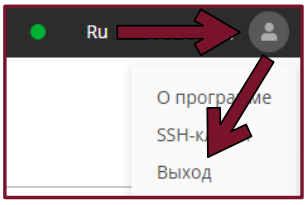

Рис. 17

4.3. Раздел «Дашборды».

4.3.1. Общая информация

Раздел «Дашборды» предоставляет статистическую информацию, регистрируемую в процессе функционирования eSensor, в удобном для пользователя виде.

Раздел «Дашборды» представлен на рис. 18.

Раздел «Дашборды»

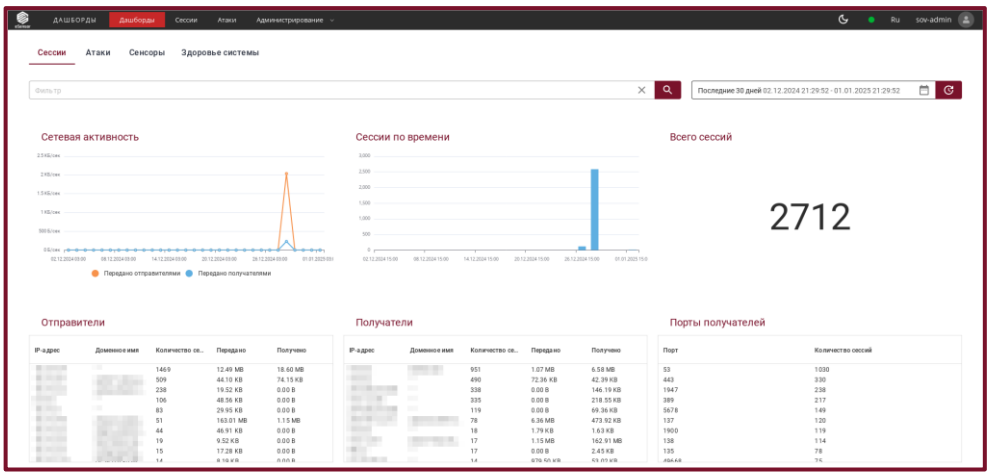

Рис. 18

Раздел «Дашборды» для удобства взаимодействия подразделяется на следующие вкладки:

– «Сессии»;

– «Атаки»;

– «Сенсоры»;

– «Здоровье системы».

4.3.2. Вкладка «Сессии»

Вкладка «Сессии» (рис. 19) предназначена для отображения отфильтрованной пользователем статистической информации о зарегистрированной сенсорами сетевой активности. Данные на вкладке отображаются в графическом и табличном виде.

Вкладка «Сессии»

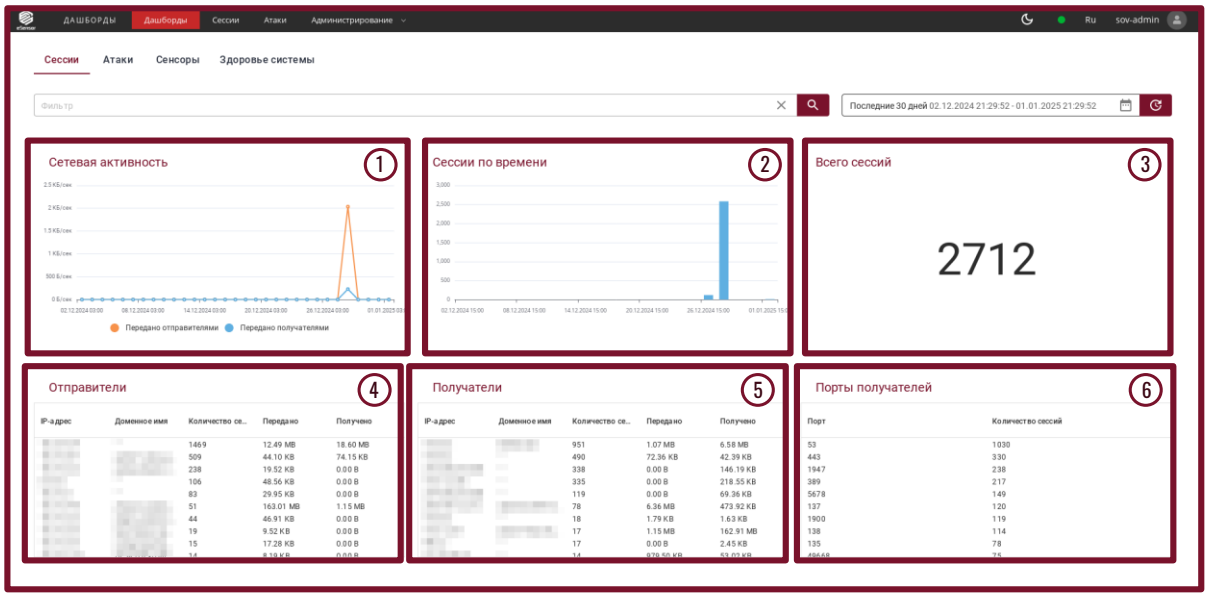

Рис. 19

Вкладка «Дашборды» содержит в себе следующие виджеты:

1) «Сетевая активность» – виджет предназначен для удобного отображения изменений средней скорости передачи отправленного и полученного трафика за установленный промежуток времени;

2) «Сессии по времени» – виджет предназначен для удобного отображения количества сессий за установленный промежуток времени;

3) «Всего сессий» – виджет предназначен для удобного отображения общего количество сессий за установленный промежуток времени;

4) «Отправители» – виджет, представляющий собой информационную таблицу, где отображается список отправителей с указанием числа сессий и объема переданного и полученного трафика за установленный промежуток времени;

5) «Получатели» – виджет, представляющий собой информационную таблицу, где отображается список получателей с указанием числа сессий, объема переданного и полученного трафика за установленный промежуток времени;

6) «Порты получателей» – виджет, представляющий собой информационную таблицу, где отображается список портов получателей сессий с указанием количества сессий за установленный промежуток времени.

В виджетах «Сетевая активность» и «Сессии по времени» число столбцов (точек) и интервал времени между столбцами (точками) рассчитываются eSensor автоматически и могут варьироваться в зависимости от установленного пользователем промежутка времени (см. п. 4.1.4 настоящего документа).

В виджетах: «Отправители», «Получатели» и «Порты получателей» информация отсортирована по количеству сессий по убыванию (от наибольшего к меньшему количеству сессий). Другие варианты сортировки не предусмотрены. Максимальное количество записей в данных виджетах – 50.

4.3.3. Вкладка «Атаки»

Вкладка «Атаки» (рис. 20) предназначена для отображения отфильтрованной пользователем статистической информации о зарегистрированных сенсорами сетевых атаках. Данные на вкладке отображаются в графическом и табличном виде.

Вкладка «Атаки»

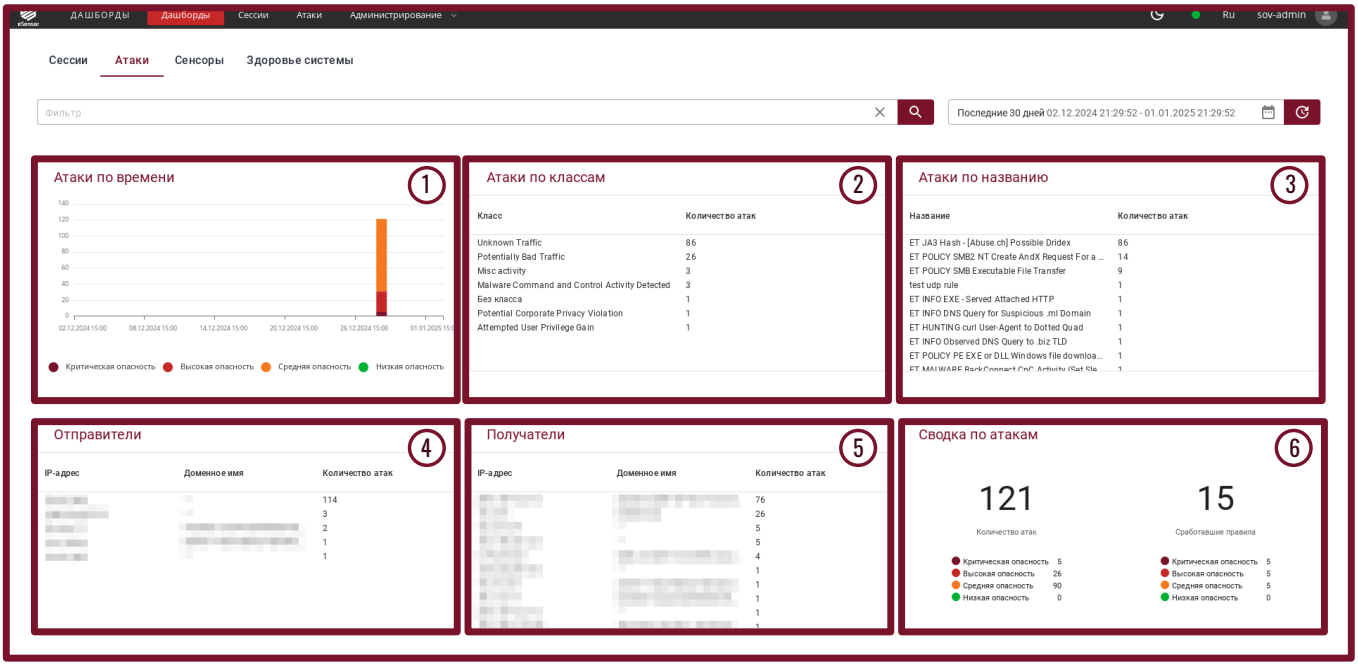

Рис. 20

Вкладка «Атаки» содержит в себе следующие виджеты:

1) «Атаки по времени» – виджет предназначен для удобного отображения количества атак каждого уровня опасности, обнаруженных за установленный промежуток времени;

2) «Атаки по классам» – виджет предназначен для удобного отображения списка классов атак с указанием количества атак каждого класса, обнаруженных за установленный промежуток времени;

3) «Атаки по названию» – виджет предназначен для удобного отображения списка названий атак с указанием их количества, обнаруженных eSensor за установленный промежуток времени;

4) «Отправители» – виджет предназначен для удобного отображения списка отправителей атак с указанием количества атак, обнаруженных за установленный промежуток времени;

5) «Получатели» – виджет предназначен для удобного отображения списка получателей атак с указанием количества атак, обнаруженных за установленный промежуток времени;

6) «Сводка по атакам» – виджет предназначен для удобного отображения общих собранных данных в цифрах об атаках, обнаруженных за установленный промежуток времени и сработавших правилах eSensor.

В виджете «Атаки по времени» число столбцов с атаками и интервал времени между столбцами рассчитываются eSensor автоматически и могут варьироваться в зависимости от установленного пользователем промежутка времени (см. п. 4.1.4 настоящего документа).

В виджетах «Атаки по времени» и «Сводка по атакам» для визуального представления различного уровня опасности атак используются следующие иконки:

– «  » – означающая критическую опасность;
– «  » – означающая высокую опасность;
– «  » – означающая среднюю опасность;
– «  » – означающая низкую опасность.

В виджетах: «Атаки по классам», «Атаки по названию», «Отправители» и «Получатели» информация отсортирована по количеству атак по убыванию (от наибольшего к меньшему количеству атак). Другие варианты сортировки не предусмотрены. Максимальное количество записей в данных виджетах – 50.

4.3.4. Вкладка «Сенсоры»

Вкладка «Сенсоры» (рис. 21) предназначена для отображения информации о работе подключенных пользователем к eSensor сенсорах. Данные на вкладке отображаются в табличном виде.

Вкладка «Сенсоры»

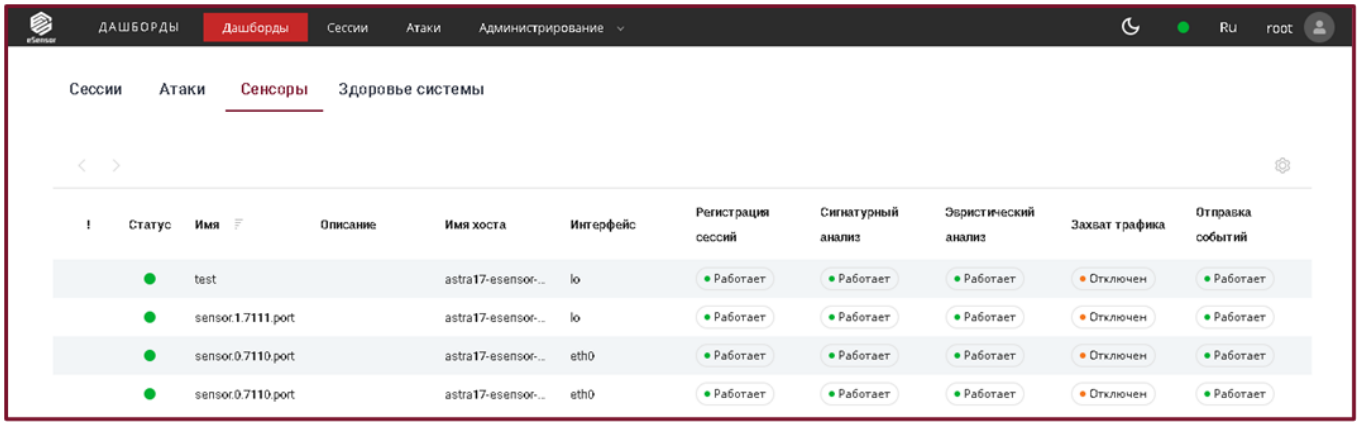

Рис. 21

Информационная таблица «Сенсоры» содержит следующую информацию:

– « **!** » – отображает индикатор предупреждения «» в случае, когда сенсором со статусом подключения «» используется **не последняя версия** группы правил. Подсказка активируется наведением курсора на иконку (см. рис. 22);

– «Статус» – отображает индикатор общего состояния подключения СУС к сенсору. Данный статус связан с индикатором общего состояния подключения СУС в карточке выбранного сенсора (п. 4.6.2.2 настоящего документа). Для отображения общего состояния подключения СУС к выбранному сенсору используются следующие иконки:

а) «» – означающий статус «Подключен»;

б) «» – означающий статус «Добавлен»;

в) «» – означающий статус «Закрыт»;

г) «» – означающий статус «Сбой связи»;

д) «» – означающий статус «Не определен».

– «Имя» – отображает название сенсора, присвоенное ему пользователем;

– «Описание» – отображает описание сенсора, заданное пользователем;

– «Имя хоста» – отображает наименование хоста подключенного сенсора и номер порта;

– «Интерфейс» – отображает название сетевого интерфейса, трафик которого захватывает и анализирует сенсор;

– «Регистрация сессий» – отображает состояние модуля регистрации сессий;

– «Сигнатурный анализ» – отображает состояние модуля сигнатурного анализа;

– «Эвристический анализ» – отображает состояние модуля эвристического анализа;

– «Захват трафика» – отображает состояние модуля захвата трафика;

– «Отправка событий» – отображает состояние модуля отправки событий ИБ.

Работа индикатора предупреждения «⚠»

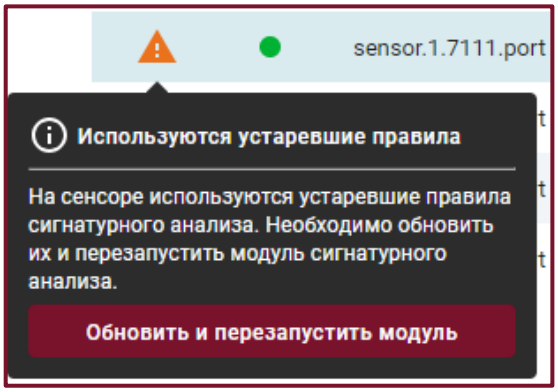

Рис. 22

Модули сенсора могут находится в одном из следующих состояний:

– «Работает» – функционирует в штатном режиме;

– «Запускается» – идет процесс запуска работы модуля;

– «Останавливается» – идет процесс остановки работы модуля;

– «Отключен» –функционирование модуля остановлено штатно;

– «Ошибка» – функционирование модуля остановлено не штатно, в следствии каких-либо ошибок;

– «Не определен» – состояние модуля неизвестно.

Функция добавления нового сенсора доступна на вкладке выпадающего меню «Администрирование» → «Сенсоры».

4.3.5. Вкладка «Здоровье системы»

Вкладка «Здоровье системы» (рис. 23) предназначена для наглядного отображения статистики работы компонентов изделия и является инструментом мониторинга состояния системы.

Вкладка «Здоровье системы»

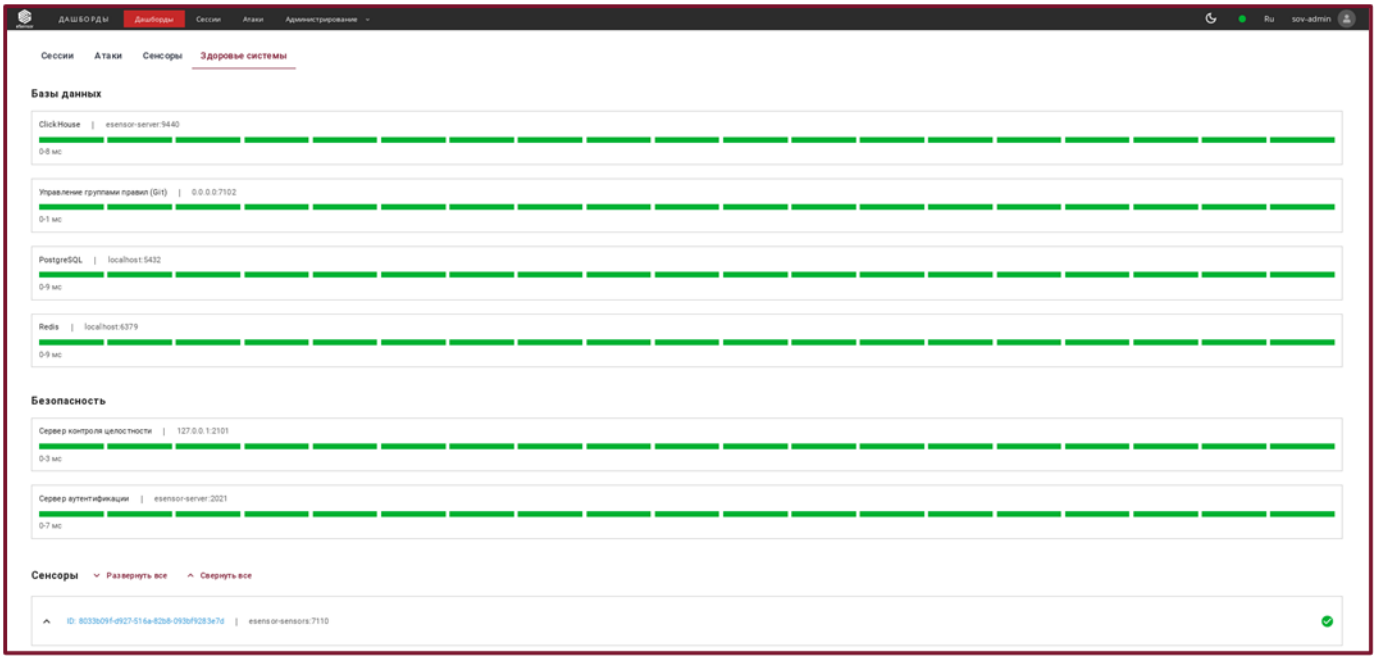

Рис. 23

Для каждого компонента изделия предусмотрена своя область с отображением строки состояний этого компонента. Строка состояний компонента представляет собой наглядное отображение изменения доступности компонента по времени. Каждому промежутку времени соответствует свое деление шкалы времени, которое может быть окрашено в следующие цвета:

– «» – компонент работает / запускается / останавливается штатно, проблем с его доступностью зафиксировано не было;

– «» – компонент отключен в данный период времени (для модулей сенсоров);

– «[redacted]» – компонент был недоступен (не определен / ошибка) в данный промежуток времени. При возникновении данного статуса компонента информация об этом отобразится в информационной панели «Последние проблемы» (рис. 3).

Компоненты сгруппированы по следующим функциональным признакам:

– группа «База данных», которая содержит информацию о компонентах:

а) «ClickHouse»;

б) «Управление группами правил (Git)»;

в) «PostgreSQL»;

г) «Redis».

– группа «Безопасность», которая содержит информацию о компонентах:

а) «Сервер контроля целостности»;

б) «Сервер аутентификации».

– группа «Сенсоры» (рис. 24), которая содержит информацию об общем состоянии сенсора, а также состоянии модулей, а именно:

а) «Общее состояние»;

б) «Регистрация сессий»;

в) «Сигнатурный анализ»;

г) «Эвристический анализ»;

д) «Захват трафика»;

е) «Отправка событий»;

ж) «Мониторинг системы» (модуль, собирающий метрики для виджетов загрузки системы).

Группа «Сенсоры»

Рис. 24

О каждом компоненте eSensor отображается следующая информация:

– название компонента (для сенсора – это id сенсора, для его модулей – название модуля) и в правой части строки индикатор «» (при общем состоянии компонентов без ошибок) или индикатор «», с цифрой количества проблем внутри него;

– адрес и порт сервиса (кроме модулей сенсора);

– строка состояний компонента, состоящая из последних 19 зарегистрированных статусов состояний компонента.

При наведении курсора на соответствующее деление шкалы времени в строке состояния компонента отобразится краткая информация о дате и времени проверки и времени ответа компонента (рис. 25).

Отображение краткой информации в выбранной шкале деления

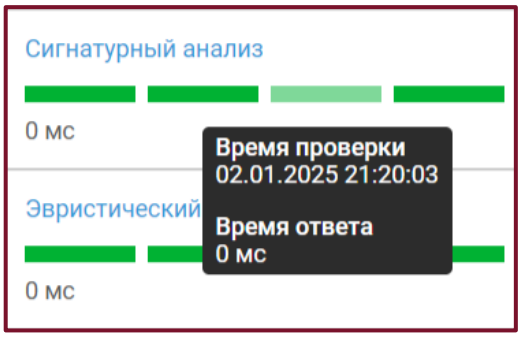

Рис. 25

При нажатии на id сенсора или названии его модуля произойдет переход в карточку сенсора (п. 4.6.2.2 настоящего документа).

eSensor проверяет общее состояние сенсоров и модулей сенсоров каждые 15 секунд, а других компонентов – каждые 30 секунд. Общее состояние рассчитывается на основе истории всех состояний контролируемых компонентов.

4.4. Раздел «Сессии»

4.4.1. Общая информация

Сенсоры разбирают поступающий на них для анализа сетевой трафик по протоколам и регистрируют информацию о сессиях – сетевых взаимодействиях между узлами сети. Данная информация может быть полезна при поиске следов вредоносной активности и расследовании атак, т.к. позволяет составить более полное представление о том, что происходит в сети.

Раздел «Сессии» предназначен для отображения информации о зарегистрированных сессиях. Информация отображается в таблице «Сессии», где каждая строка – это различные данные одной сессии, а каждый столбец – тип данных, относящийся к заголовку данной таблицы.

Раздел «Сессии» представлен на рис. 26.

Раздел «Сессии»

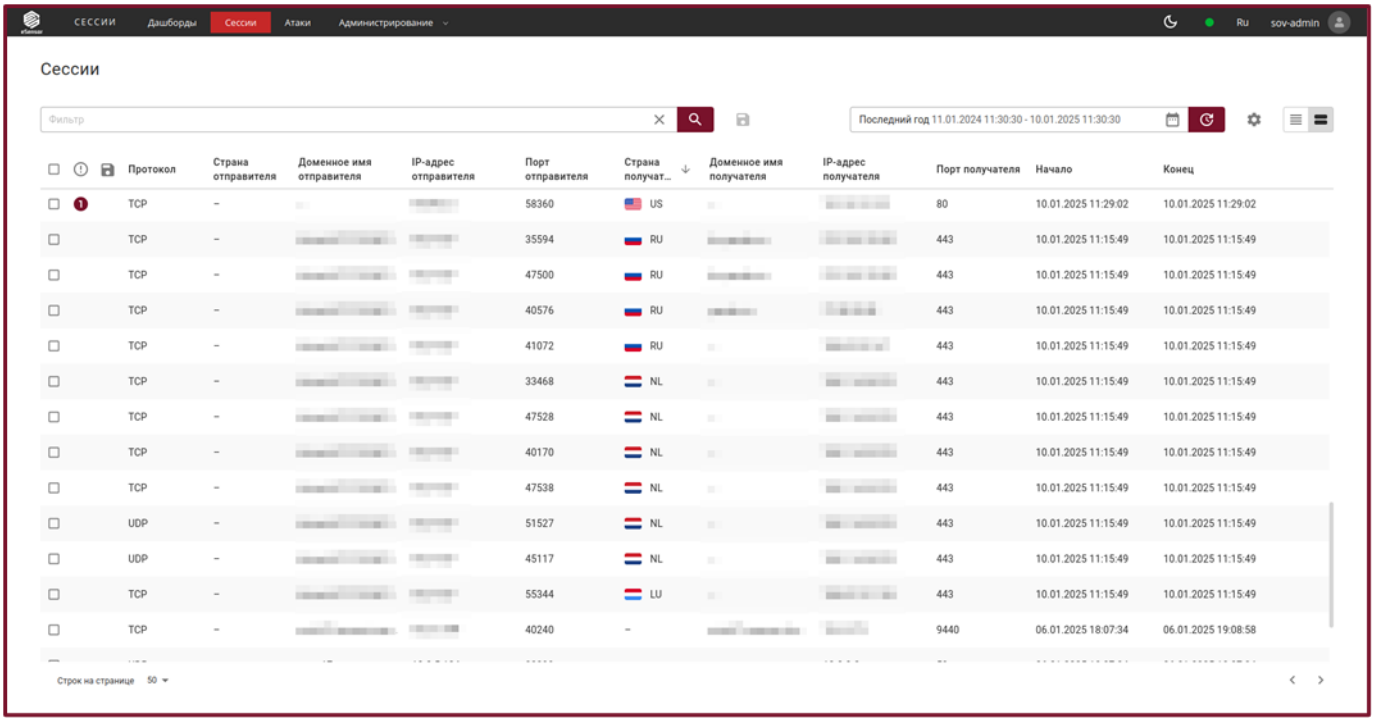

Рис. 26

При нажатии курсором на интересующую строку информационной таблицы «Сессии» произойдет переход к карточке выбранной сессии (п. 4.4.4 настоящего документа).

4.4.2. Управление отображением информации о сессиях

Управление отображением информации о сессиях, фильтрация по специальным выражениям и по времени, поиск подробно описаны в п. 4.1 настоящего документа.

4.4.3. Копирование дампов сессии в хранилище

Сенсор записывает дампы регистрируемых им сессий в заданную папку файловой системы машины, на которую он установлен.

Примечание. Настройки записи и хранения дампов на сенсоре задаются в подменю «Регистрация сессий» карточки сенсора (п. 4.6.2.2.1 настоящего документа).

Чтобы не потерять важный дамп при автоматической очистке папки с дампами, а также иметь возможность скачать его из eSensor на компьютер, нужно скопировать его в хранилище PCAP-файлов на СУС.

Примечание. Работа с хранилищем PCAP-файлов на СУС описана в п. 4.6.3 настоящего документа.

Для копирования одного/нескольких дампов сессий в хранилище необходимо создать запрос/запросы на копирование.

«» – это кнопка «Создать запрос на копирование дампов», которая по умолчанию неактивна. Становится доступна при выборе одной или нескольких сессий путем активации чекбоксов в необходимых строках в информационной таблице «Сессии».

Для копирования дампов сессий из информационной таблицы «Сессии» необходимо выбрать интересующие сессии, активировав чекбоксы в необходимых строках и нажать кнопку «» над информационной таблицей «Сессии».

После нажатия на кнопку «» откроется окно «Создание запроса на копирование дампов» (пример см. на рис. 27).

Окно «Создание запроса на копирование дампов»

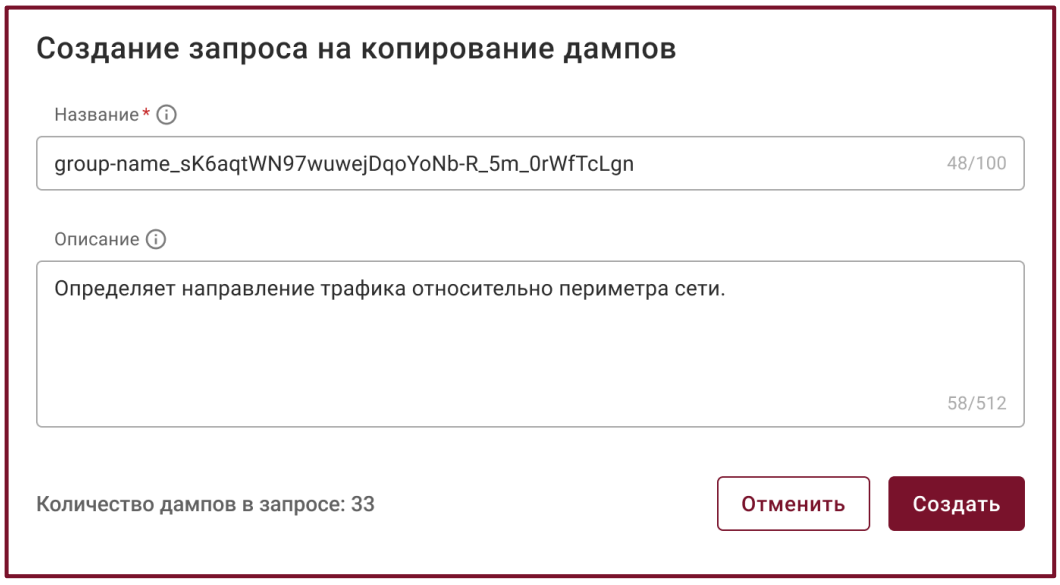

Рис. 27

В окне «Создание запроса на копирование дампов» необходимо заполнить следующее:

– «Название» – название запроса может содержать произвольные символы. Обязательное поле для заполнения. Если было выбрано более одного дампа, то каждому будет присвоено имя в следующем формате: **<name>_<id>**, где: <name> – название, а <id> – целочисленный идентификатор каждого дампа, начиная с 1;

– «Описание» – может содержать произвольные символы. В случае выбора нескольких дампов сессии в создаваемом запросе данное описание будет присвоено каждому.

Примечание. При выборе нескольких дампов сессии в создаваемом запросе – в левом нижнем углу окна «Создание запроса на копирование дампов» будет указано количество выбранных ранее дампов в запросе. В таком случае будет создана группа запросов. Число запросов в группе будет равно числу копируемых дампов.

Далее, для отмены создания запроса необходимо нажать кнопку «Отменить» или для подтверждения введенных данных нажать кнопку «Создать». После успешного создания запроса eSensor предложит пользователю нажатием кнопки «Перейти» совершить быстрый переход к странице с информацией о запросах (рис. 28), а именно на вкладку «Запросы на копирование» выпадающего меню «Администрирование» (п. 4.6.4 настоящего документа). При отсутствии такой необходимости следует нажать кнопку «Отменить» для возврата к разделу «Сессии».

Окно подтверждения успешно созданного запроса

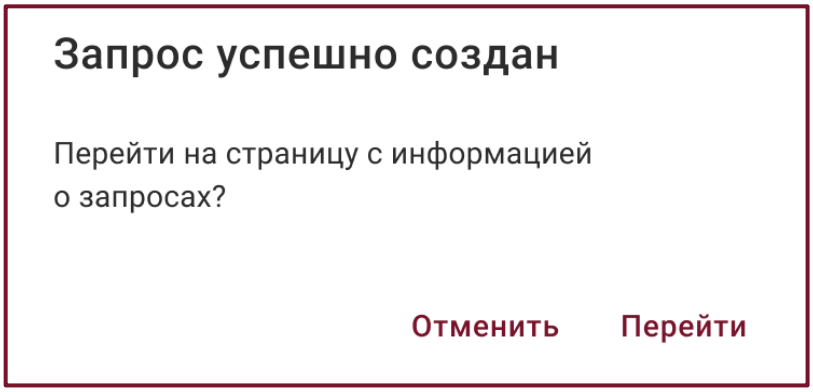

Рис. 28

4.4.4. Карточка сессии

4.4.4.1. Общее описание

В eSensor предусмотрена возможность просмотра подробной информации о сессии. Для этой цели служит карточка сессии. Для перехода к карточке сессии необходимо нажать на строку таблицы сессий в любом месте.

После нажатия на строку в таблице сессий отобразится страница карточки этой сессии (рис. 29).

Карточка выбранной сессии

Рис. 29

Страницу «Карточка сессии» можно разделить на следующие функциональные блоки:

– «График»;

– «Информация о сессии»;

– «Атаки».

4.4.4.2. Блок «График»

В верхнем блоке карточки сессии отображается график скорости трафика в сети (поле «Сетевая активность»). Над данным полем указываются IP-адреса и порты отправителя и получателя информации.

Так же в eSensor предусмотрена возможность отключения отображения полученного или отправленного трафика. Для отключения отображения принятого трафика необходимо нажать на надпись «Полученный трафик» над графиком скорости сетевого трафика, для отключения отображения отправленного трафика – на надпись «Отправленный трафик». Для включения отображения принятого или отправленного трафика необходимо снова нажать на соответствующую надпись.

Для выбора единиц измерения скорости сетевого трафика необходимо нажать на поле в правом верхнем углу блока графика скорости сетевого трафика (поле с надписью «Байты/сек») и в открывшемся списке выбрать масштаб отображения скорости трафика. После чего график скорости сетевого трафика будет перестроен в соответствии с выбранными параметрами.

Под навигационной шкалой блока графика скорости сетевого трафика расположена строка основной информации о трафике на текущем участке графика сессии, включающая следующую информацию:

– общий трафик;
– количество переданной информации;
– количество полученной информации;
– средняя скорость передачи данных.

За время существования сессии на узел исследуемой сети могут совершаться атаки. В eSensor предусмотрена функция отображения атак на узел исследуемой сети, зарегистрированных сенсорами за время существования сессии, карточку которой просматривает оператор.

Для отображения графика атак, зарегистрированных за время существования сессии, необходимо нажать на надпись «Сетевая активность», появится выпадающий список, где необходимо выбрать «Атаки».

График атак показывает распределение интенсивности атак, совершаемых на узел исследуемой сети, за время существования сессии. График представляется в виде столбцов, находящихся на временной шкале в те моменты, когда атаки были зарегистрированы сенсором/сенсорами. Каждый столбец представляет собой набор атак разных уровней критичности. Таким образом, высота столбца указывает на общее количество атак, зарегистрированных в конкретный момент времени существования сессии. Под навигационной шкалой указывается количество атак каждого уровня угрозы и общее количество атак, зарегистрированных за время существования сессии.

Управление графиком распределения интенсивности атак аналогично управлению графиком скорости сетевого трафика. При наведении курсора мыши на какой-либо столбец в eSensor отображается прозрачное всплывающее окно с подробным описанием количества атак по уровням критичности.

4.4.4.3. Блок «Информация о сессии»

Данный блок служит для отображения подробной информации о сессии. Представляются следующие данные:

– общая информация:

а) «Протокол» – использованный протокол сетевого взаимодействия;

б) «Начало» – дата и время открытия сессии;

в) «Конец» – дата и время закрытия сессии;

г) «Длительность» – продолжительность сессии;

д) «Дамп сессии» – индикатор, сохранен ли дамп сессии в хранилище PCAP-файлов на СУС;

е) «Сенсор» – информация о том, какой сенсор зарегистрировал данную сессию;

ж) «Интерфейс» – на каком сетевом интерфейсе сенсора была зарегистрирована данная сессия;

з) «Community ID» – идентификатор сессии, определенный по алгоритму Community ID;

и) «Всего передано» – общее количество переданных байтов и пакетов.

– участники сессии:

а) «Страна» – страны отправителя и получателя сетевого трафика;

б) «Доменное имя» – доменные имена отправителя и получателя сетевого трафика;

в) «IP-адрес» – IP-адреса отправителя и получателя сетевого трафика;

г) «Порт» – порты отправителя и получателя сетевого трафика, через которые была установлена сессия;

д) «Передано» – количество информации, переданное отправителем и получателем сетевого трафика.

4.4.4.4. Блок «Атаки»

Данный блок предназначен для отображения атак, зарегистрированных во время передачи данных в рамках рассматриваемой сессии, и представляет собой список этих атак.

Каждая строка списка соответствует своей зарегистрированной атаке. При нажатии на одну из строк списка атак происходит переход к карточке атаки.

В случае, если во время сессии было обнаружено много атак, они не помещаются на одной странице. Внизу блока «Атаки» предусмотрена строка навигации в списке атак.

4.5. Раздел «Атаки»

4.5.1. Общее описание

В процессе анализа сетевого трафика, проходящего через узлы исследуемой сети, сенсорами автоматически регистрируются факты совершения атак. Под атаками в eSensor понимаются срабатывания правил (п. 4.6.5 настоящего документа), кроме правил с действием «pass» – пропустить. Для перехода к разделу «Атаки» eSensor необходимо нажать на соответствующую кнопку на панели навигации.

После нажатия на кнопку «Атаки» на панели навигации eSensor произойдет переход к разделу «Атаки» (рис. 30).

Раздел «Атаки»

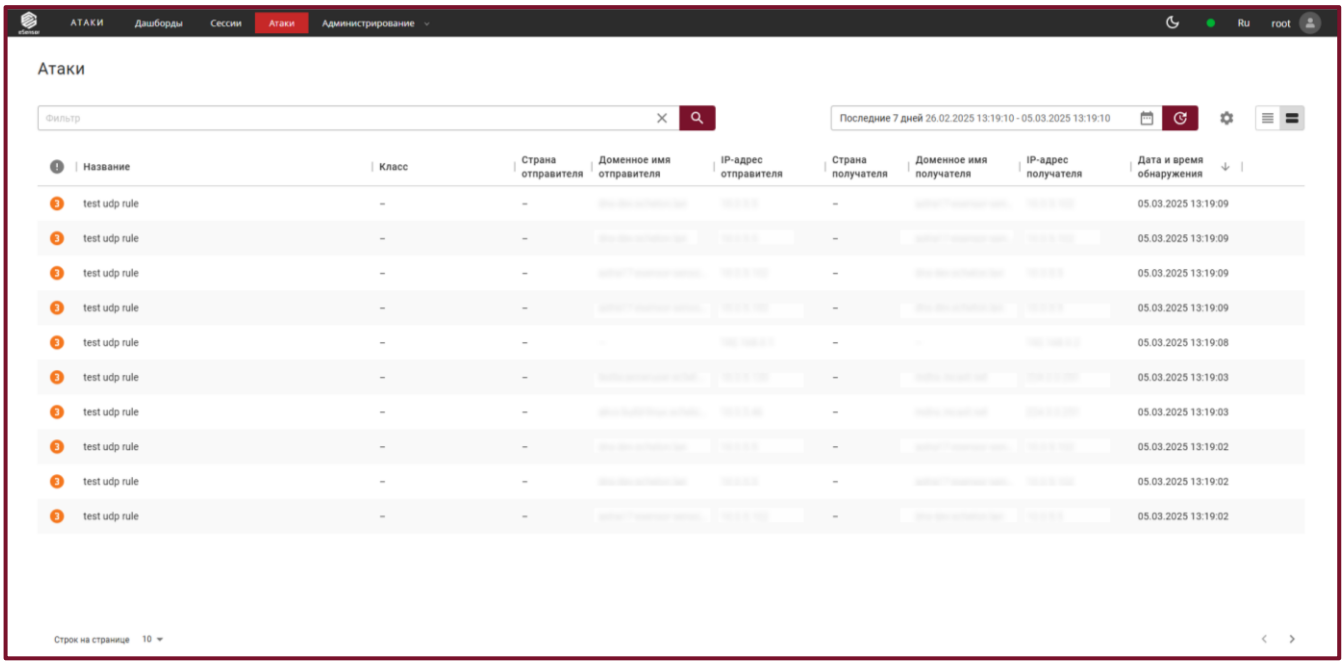

Рис. 30

Раздел «Атаки» представляет собой информационную таблицу со всеми зарегистрированными сенсорами eSensor атаками.

Раздел «Атаки» можно разбить на следующие функциональные блоки:

1) управление отображением информации об атаках eSensor;

2) поиск по фильтру;

3) информационная таблица «Атаки».

В eSensor предусмотрены следующие функции управления отображением информации об атаках:

– отображение атак за указанный период времени (поле с иконкой «»);

– управление отображением столбцов таблицы (кнопка «»).

Настройка отображения атак за указанный период времени аналогична настройке отображения сессий.

Работа зоны поиска по фильтру аналогична описанной в п. 4.1.3 настоящего документа.

Для управления отображением столбцов таблицы необходимо нажать на кнопку «» в зоне отображения информации. После чего откроется меню настройки отображения столбцов.

4.5.2. Карточка атаки

В eSensor предусмотрена возможность просмотра подробной информации о зарегистрированной атаке на узел исследуемой сети. Для этой цели служит карточка атаки.

Для перехода к карточке атаки необходимо нажать на строку таблицы атак в любом месте.

После нажатия на строку в таблице атак отобразится карточка этой атаки (рис. 31).

Карточка выбранной атаки

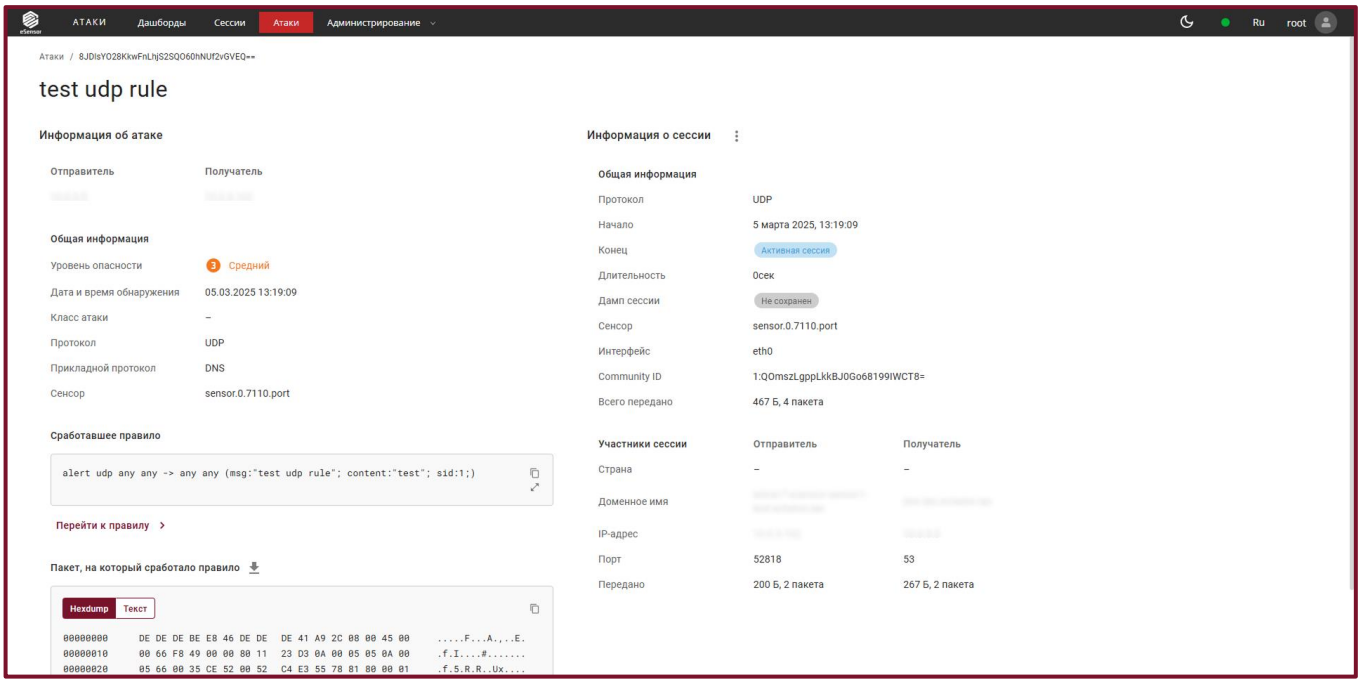

Рис. 31

4.6. Выпадающее меню «Администрирование»

4.6.1. Общая информация

Выпадающее меню «Администрирование» предоставляет доступ к дополнительным возможностям и настройкам eSensor. Для раскрытия выпадающего меню «Администрирование» необходимо нажать на одноименную вкладку на панели навигации.

При нажатии на выпадающее меню «Администрирование» отобразится список доступных инструментов eSensor, где пользователю предоставляется выбор для нажатия и открытия одной из следующих вкладок:

– «Сенсоры»;

– «Управление PCAP-файлами»;

– «Запросы на копирование»;

– «Группы правил».

4.6.2. Вкладка «Сенсоры»

4.6.2.1. Общая информация

На вкладке «Сенсоры» eSensor отображается информационная таблица, содержащая информацию о зарегистрированных в системе сенсорах (рис. 32).

Вкладка «Сенсоры»

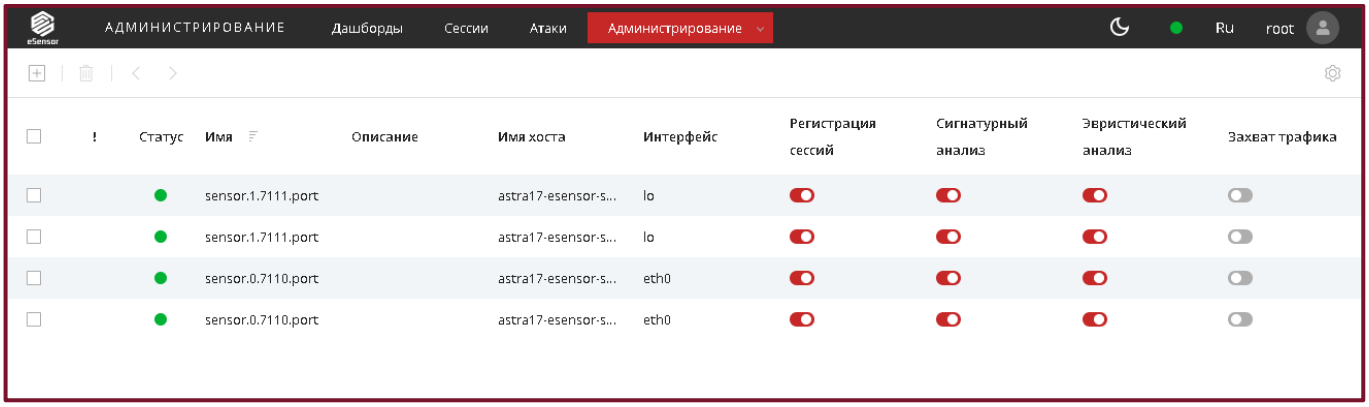

Рис. 32

Данная информационная таблица содержит ту же информацию, что и информационная таблица на вкладке «Сенсоры» раздела «Дашборды» (п. 4.3.4 настоящего документа), только вместо состояний модулей сенсоров в ней отображаются переключатели, с помощью которых можно приводить модули в состояние работы и, наоборот, отключать их.

В eSensor предусмотрена возможность просмотра подробной информации о сенсоре, зарегистрированном в системе. Для этого необходимо кликнуть в любом месте строки информационной таблицы сенсоров, соответствующей информации об интересующем сенсоре. После чего произойдет переход к карточке выбранного сенсора.

4.6.2.2. Карточка сенсора

В eSensor предусмотрена возможность просмотра подробной информации о выбранном сенсоре. Для этой цели служит карточка сенсора (рис. 33).

Карточка выбранного сенсора

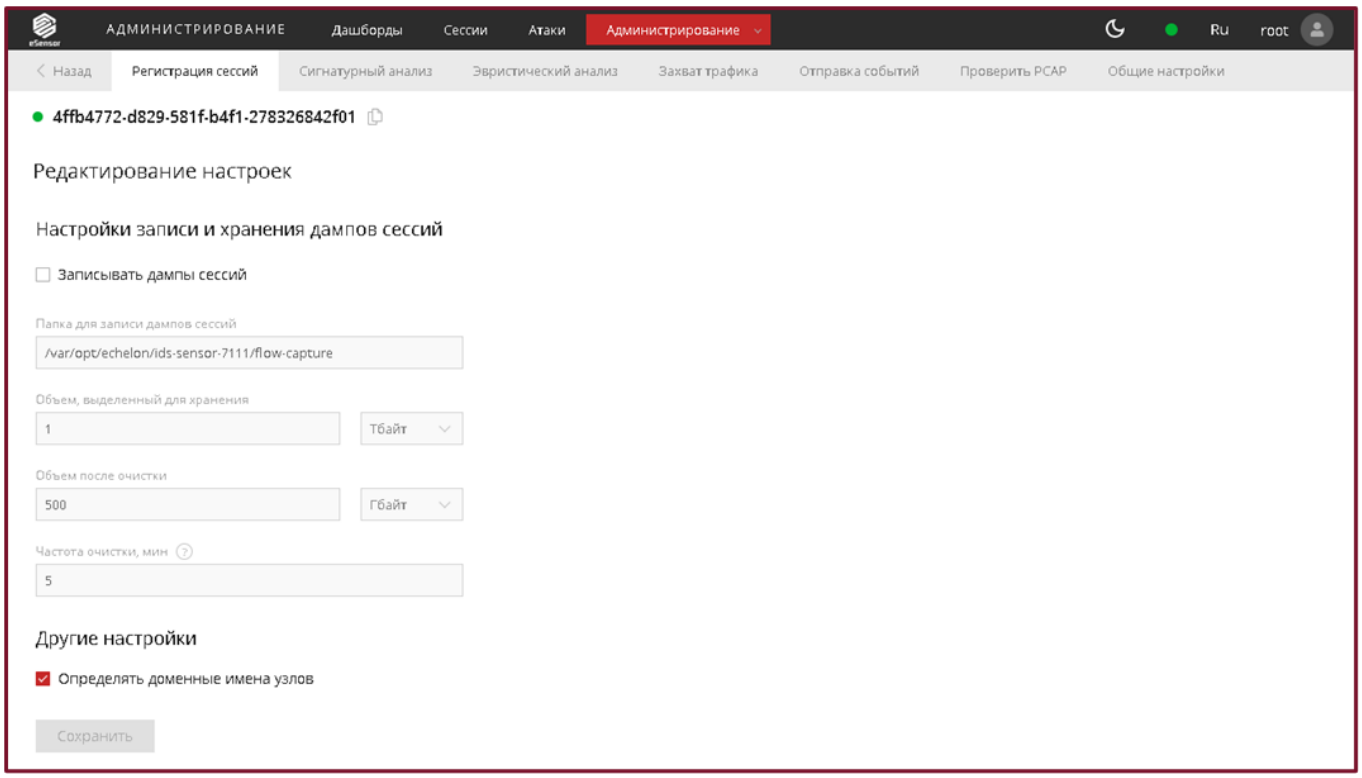

Рис. 33

Карточка сенсора содержит следующие подменю и вкладки с информацией о данном сенсоре:

– подменю «Регистрация сессий»;

– подменю «Сигнатурный анализ»:

а) вкладка «Настройки»;

б) вкладка «Логи»;

в) вкладка «Группы узлов»;

г) вкладка «Группы портов».

– подменю «Эвристический анализ»:

а) вкладка «Настройки»;

б) вкладка «Логи».

– подменю «Захват трафика»:

а) вкладка «Настройки»;

б) вкладка «Логи».

– подменю «Отправка событий»:

а) вкладка «Настройки»;

б) вкладка «Логи».

– подменю «Проверить PCAP»;

– подменю «Общие настройки».

4.6.2.2.1. Подменю «Регистрация сессий»

Управление модулем регистрации сессий сенсора осуществляется на странице «Администрирование» → «Сенсоры» → «Сенсор» → «Регистрация сессий».

Подменю «Регистрация сессий» карточки сенсора представлено на рис. 34.

Подменю «Регистрация сессий» карточки сенсора

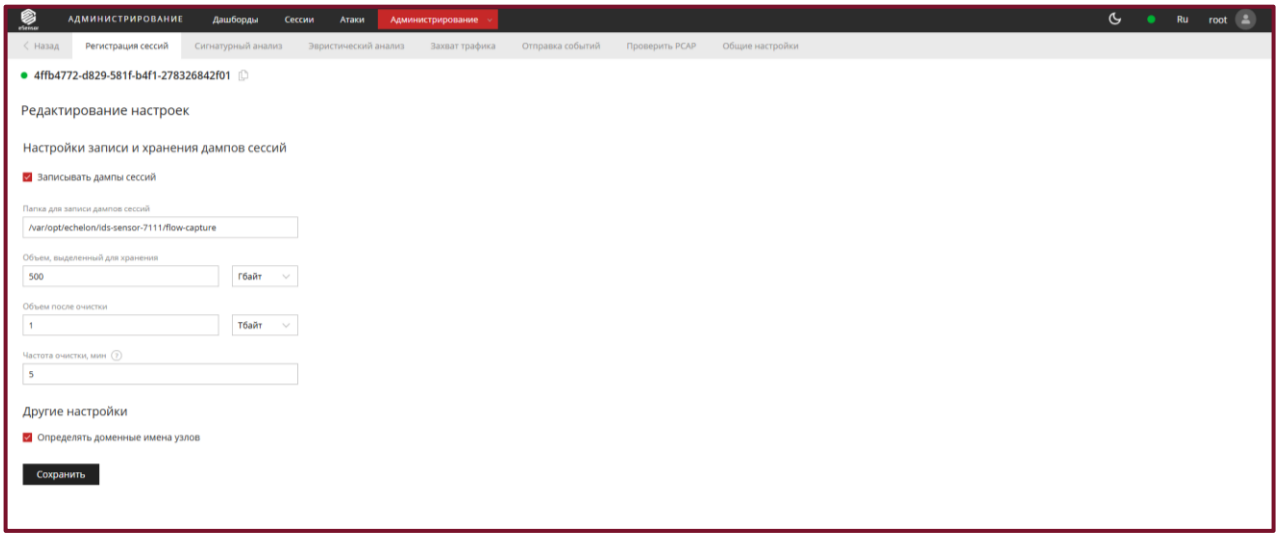

Рис. 34

Активная настройка «Записывать дампы сессий» включает функцию записи и хранения дампов регистрируемых сенсором сетевых сессий в соответствии с параметрами, задаваемыми в полях, описание которых приведено в таблице 2.

Таблица 2 – Настройки записи и хранения дампов сессий

Поле	Описание и возможные значения	Пример
Папка для записи дампов сессий	Папка для записи дампов сессий в файловой системе машины, на которой установлен сенсор	`/var/opt/echelon/ids-sensor-7110/flow-capture`
Объем, выделенный для хранения	Объем, выделенный для хранения записываемых дампов сессий	2 (Тбайт)
Объем после очистки	Объем дампов сессий после очистки	1 (Тбайт)
Частота очистки, мин	Частота, с которой система будет проверять, не превышает ли совокупный объем хранящихся дампов сессий объема, выделенного для хранения	5

Через интервал времени **«Частота очистки, мин»** будет происходить проверка, не превышен ли **«Объем, выделенный для хранения»**. Если превышен, будет произведена очистка. При этом будут удалены самые старые файлы с записанным трафиком. Будет удалено столько файлов, сколько необходимо, чтобы общий объем хранящихся дампов не превышал значения **«Объем после очистки»**.

Активная настройка «Определять доменные имена узлов» включает функцию определения доменных имен узлов сессий и атак по их IP-адресам.

4.6.2.2.2. Подменю «Сигнатурный анализ»

Управление модулем сигнатурного анализа сенсора осуществляется на странице «Администрирование» → «Сенсоры» → «Сенсор» → «Сигнатурный анализ».

Подменю «Сигнатурный анализ» карточки сенсора представлено на рис. 35.

Подменю «Сигнатурный анализ» карточки сенсора

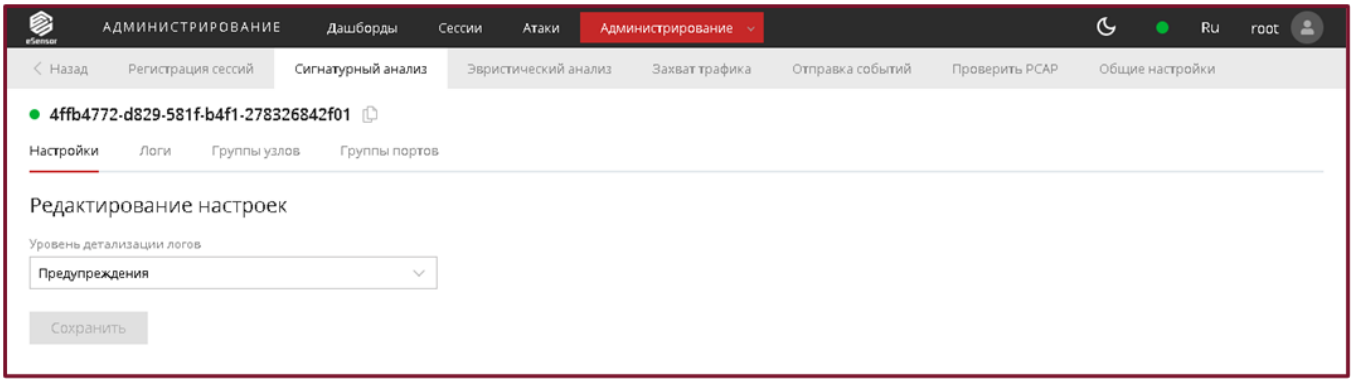

Рис. 35

Подменю «Сигнатурный анализ» состоит из следующих функциональных вкладок:

– «Настройки» (см. рис. 35). Данная вкладка предназначена для просмотра и изменения настроек модуля сигнатурного анализа сенсора, а именно уровня детализации логов;

– «Логи» (см. рис. 36). Данная вкладка предназначена для отображения системного журнала модуля сигнатурного анализа сенсора eSensor;

Вкладка «Логи» подменю «Сигнатурный анализ»

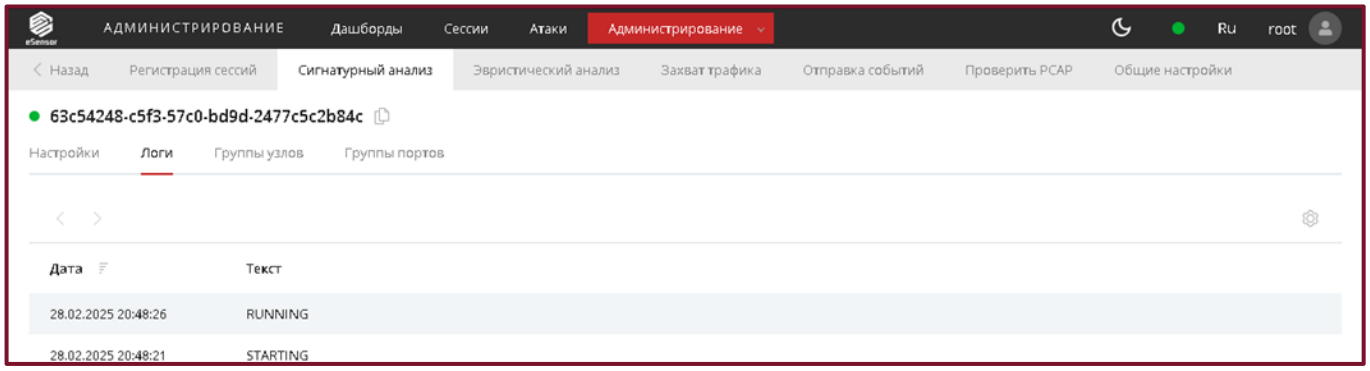

Рис. 36

– «Группы узлов» (см. рис. 37). Данная вкладка предназначена для отображения информации о группах узлов. Группы узлов – инструмент eSensor, позволяющий объединять активы исследуемой сети в группы, для которых будут применяться те или иные решающие правила обработки регистрируемых событий ИБ. У каждого сенсора есть набор групп узлов по умолчанию. При необходимости можно изменить существующие группы, удалить их или добавить новые;

Вкладка «Группы узлов» подменю «Сигнатурный анализ»

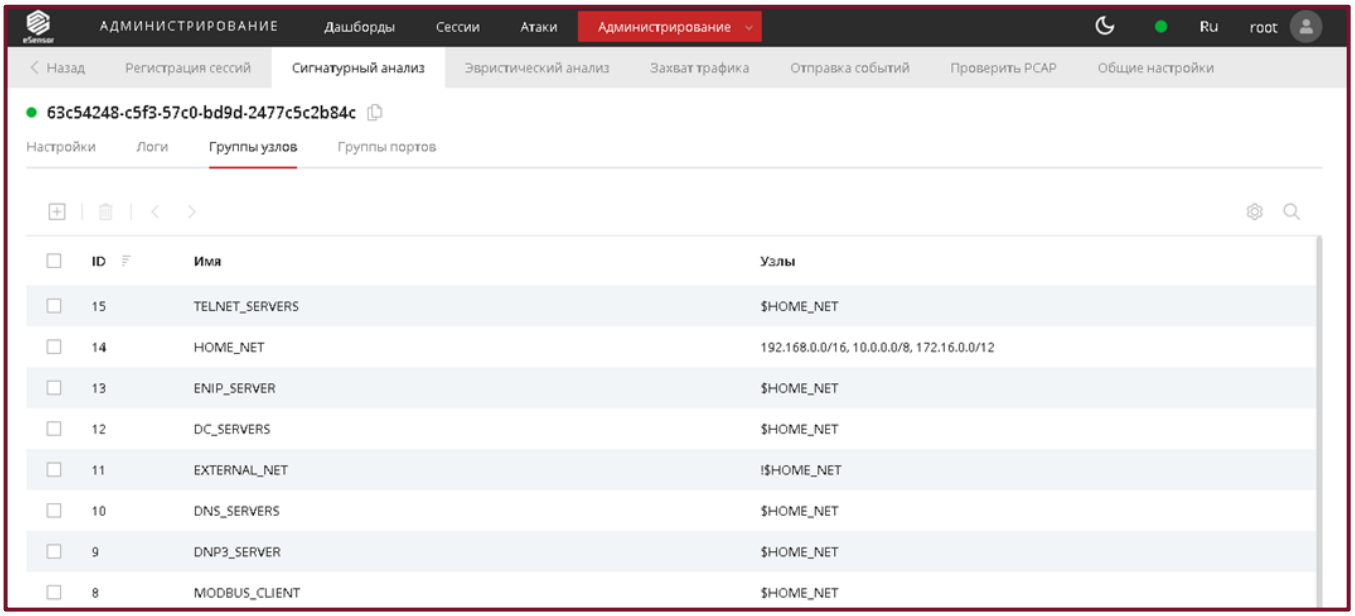

Рис. 37

– «Группы портов» (см. рис. 38). Данная вкладка подменю «Сигнатурный анализ» карточки сенсора (аналогично вкладке «Группы узлов») предназначена для отображения информации о группах портов. У каждого сенсора есть набор групп портов по умолчанию. При необходимости можно изменить существующие группы, удалить их или добавить новые.

Вкладка «Группы портов» подменю «Сигнатурный анализ»

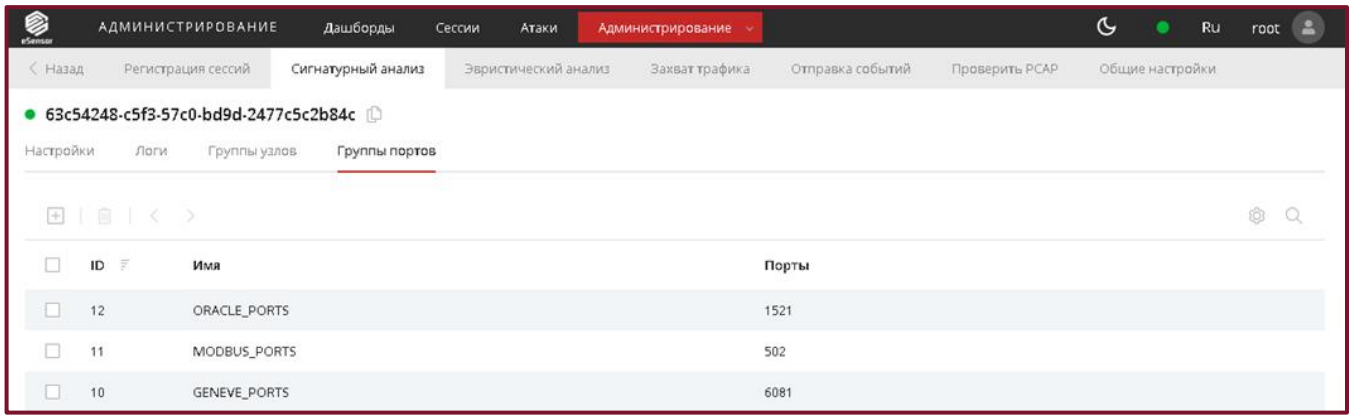

Рис. 38

Настройка модуля

Вкладка «Настройки» предоставляет возможность задавать настройки модуля, описанные в таблице 3.

Таблица 3 – Настройки модуля сигнатурного анализа

Поле	Описание и возможные значения	Пример
Уровень детализации логов	Уровень детализации записей в системном журнале модуля сигнатурного анализа (вкладка «Логи»). Возможные значения (по возрастанию уровня детализации): – «Ошибки»; – «Предупреждения»; – «Оповещения»; – «Информирование»; – «Производительность»; – «Конфигурация»; – «Отладка»	Предупреждения

Просмотр системного журнала модуля

В eSensor ведется системный журнал модуля сигнатурного анализа, в который записывается информация об ошибках и другая диагностическая информация, регистрируемая во время запуска, выполнения и выключения модуля.

Для просмотра системного журнала модуля необходимо перейти на вкладку «Логи» страницы «Администрирование» → «Сенсоры» → «Сенсор» → «Сигнатурный анализ».

Данная вкладка позволяет:

– просматривать таблицу с записями системного журнала модуля;

– настраивать таблицу с записями системного журнала модуля.

В рабочей области страницы находится информационная таблица с записями системного журнала модуля. По умолчанию каждая запись содержит информацию, указанную в таблице 4.

Таблица 4 – Информация в записях системного журнала модуля сигнатурного анализа

Столбец	Описание
Дата	Дата и время создания записи в журнале
Текст	Содержимое записи

Создание группы узлов

Для создания группы узлов необходимо нажать кнопку « ⊞ », заполнить поля появившейся формы (рис. 39) и нажать кнопку «Сохранить».

Форма создания группы узлов

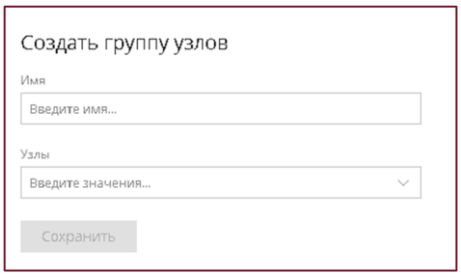

Рис. 39

Форма создания группы узлов состоит из полей, указанных в таблице 5.

Таблица 5 – Поля формы создания группы узлов

Поле	Описание и возможные значения	Пример
Имя	Имя группы. Обязательное поле	HOME_NET
Узлы	Узлы, которые должны быть включены в группу. Обязательное поле	10.0.5.0/24

Просмотр карточки группы узлов

Для редактирования группы узлов необходимо перейти в карточку группы (рис. 40), кликнув по строке с информацией о данной группе, внести требуемые изменения в поля карточки (поля представлены в таблице 5) и нажать «Сохранить».

Форма создания группы узлов

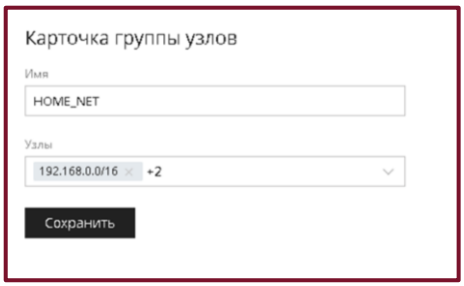

Рис. 40

Удаление группы узлов

Для удаления группы узлов необходимо выбрать группу узлов, которую требуется удалить, выставив « ☑ » в строке с информацией о данной группе, нажать кнопку « 🗑 ».

Создание группы портов

Для создания группы портов необходимо нажать кнопку « ⊞ », заполнить поля появившейся формы (рис. 41), нажать «Сохранить».

Форма создания группы портов

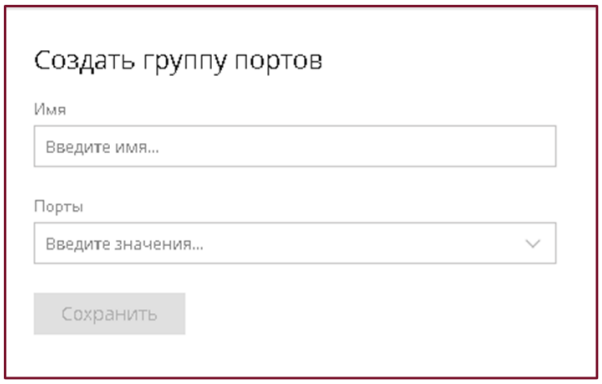

Рис. 41

Форма создания группы портов состоит из полей, указанных в таблице 6.

Таблица 6 – Поля формы создания группы портов

Поле	Описание и возможные значения	Пример
Имя	Имя группы. Обязательное поле	HOME_NET
Порты	Порты, которые должны быть включены в группу. Обязательное поле	10.0.5.0/24

Просмотр карточки группы портов

Для редактирования группы портов необходимо перейти в карточку группы (рис. 42), кликнув по строке с информацией о данной группе, внести требуемые изменения в поля карточки (поля представлены в таблице 6), нажать «Сохранить».

Карточка группы портов

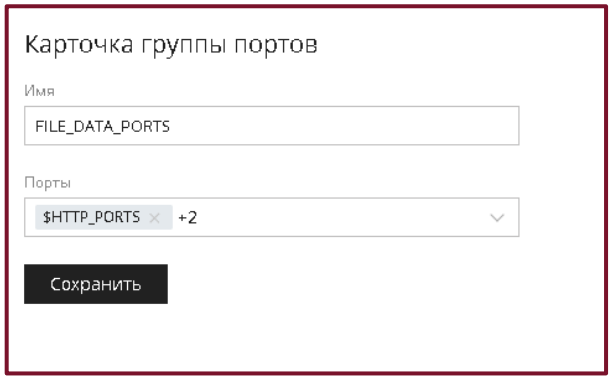

Рис. 42

Удаление группы портов

Для удаления группы портов необходимо выбрать группу портов, которую требуется удалить, « ☑ » в строке с информацией о данной группе, нажать кнопку « 🗑 ».

4.6.2.2.3. Подменю «Эвристический анализ»

Подменю «Эвристический анализ» карточки сенсора представлено на рис. 43.

Подменю «Эвристический анализ» карточки сенсора

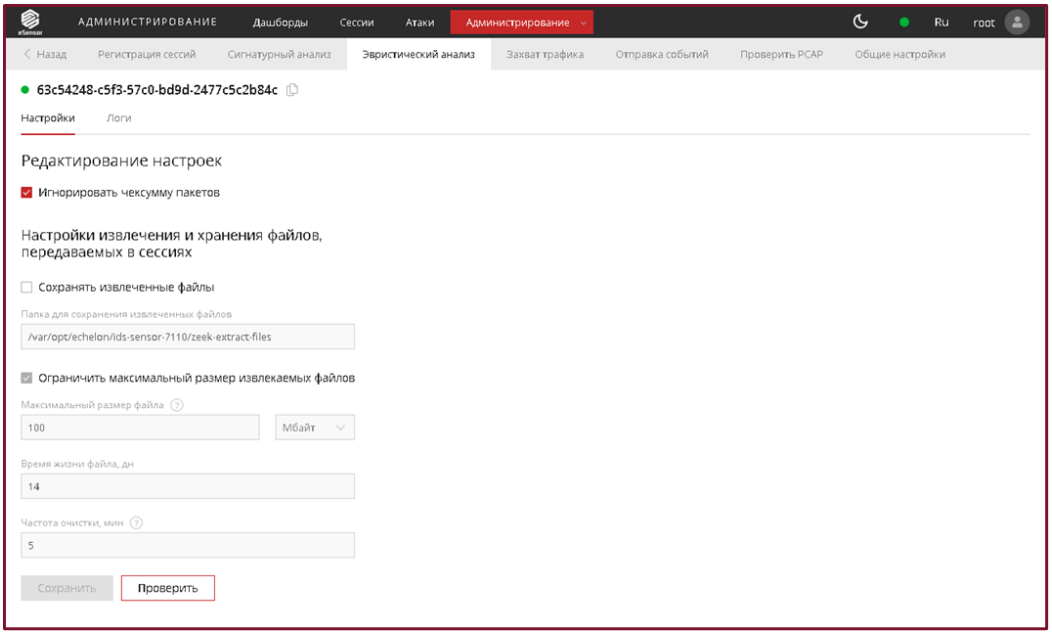

Рис. 43

Подменю «Эвристический анализ» состоит из следующих функциональных вкладок:

– «Настройки» (см. рис. 43). Данная вкладка предназначена для просмотра и редактирования настроек модуля эвристического анализа сенсора;

– «Логи» (см. рис. 44). Аналогично подменю «Сигнатурный анализ» карточки сенсора, данная вкладка предназначена для отображения системного журнала модуля эвристического анализа сенсора eSensor.

Вкладка «Логи» подменю «Эвристический анализ» карточки сенсора

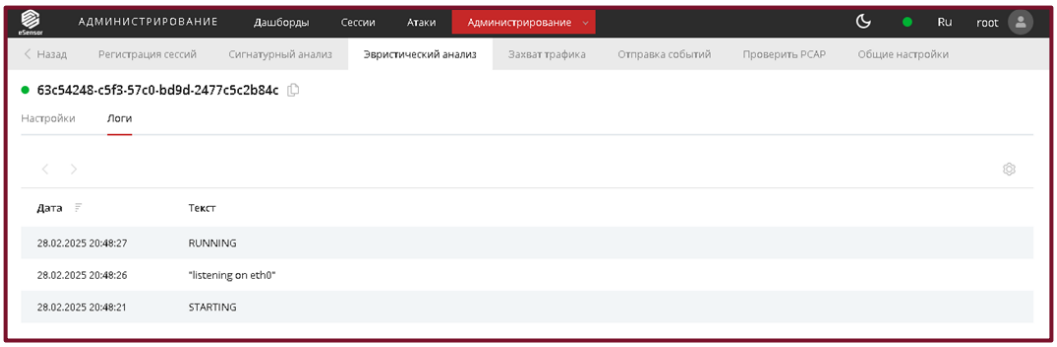

Рис. 44

Настройка модуля

Активная настройка «Не проверять контрольные суммы пакетов» указывает модулю эвристического анализа сенсора при анализе трафика игнорировать любые ошибки, связанные с контрольной суммой TCP.

В секции «Настройки извлечения и хранения файлов, передаваемых в сессиях» присутствуют следующие настройки:

– активная настройка «Сохранять извлеченные файлы» – включает функцию сохранение копий извлекаемых из сессий файлов (если данная настройка выключена, об извлеченных файлах будут регистрироваться только общие сведения, а возможность скачать файл будет недоступна);

– «Папка для сохранения извлеченных файлов» – путь в файловой системе машины с сенсором к папке, в которую необходимо сохранять извлекаемые файлы;

– активная настройка «Ограничить максимальный размер извлекаемых файлов» – позволяет задать соответствующее ограничение: если размер извлеченного файла превышает «Максимальный размер файла», будет сохранена только часть файла заданного максимального размера;

– настройки «Время жизни файла, дн» и «Частота очистки, мин» – определяют условия, по которым eSensor должен удалять старые файлы.

Например, если установить время жизни файла – 7 дней, а частоту очистки 5 минут, eSensor будет проверять каждые 5 минут, нет ли извлеченных файлов, которые хранятся уже более 7 дней. Если такие файлы есть, они будут удалены.

При изменении настроек модуля, чтобы изменения вступили в силу, необходимо нажать кнопку «Сохранить».

4.6.2.2.4. Подменю «Захват трафика»

Подменю «Захват трафика» карточки сенсора представлено на рис. 45.

Подменю «Захват трафика» карточки сенсора

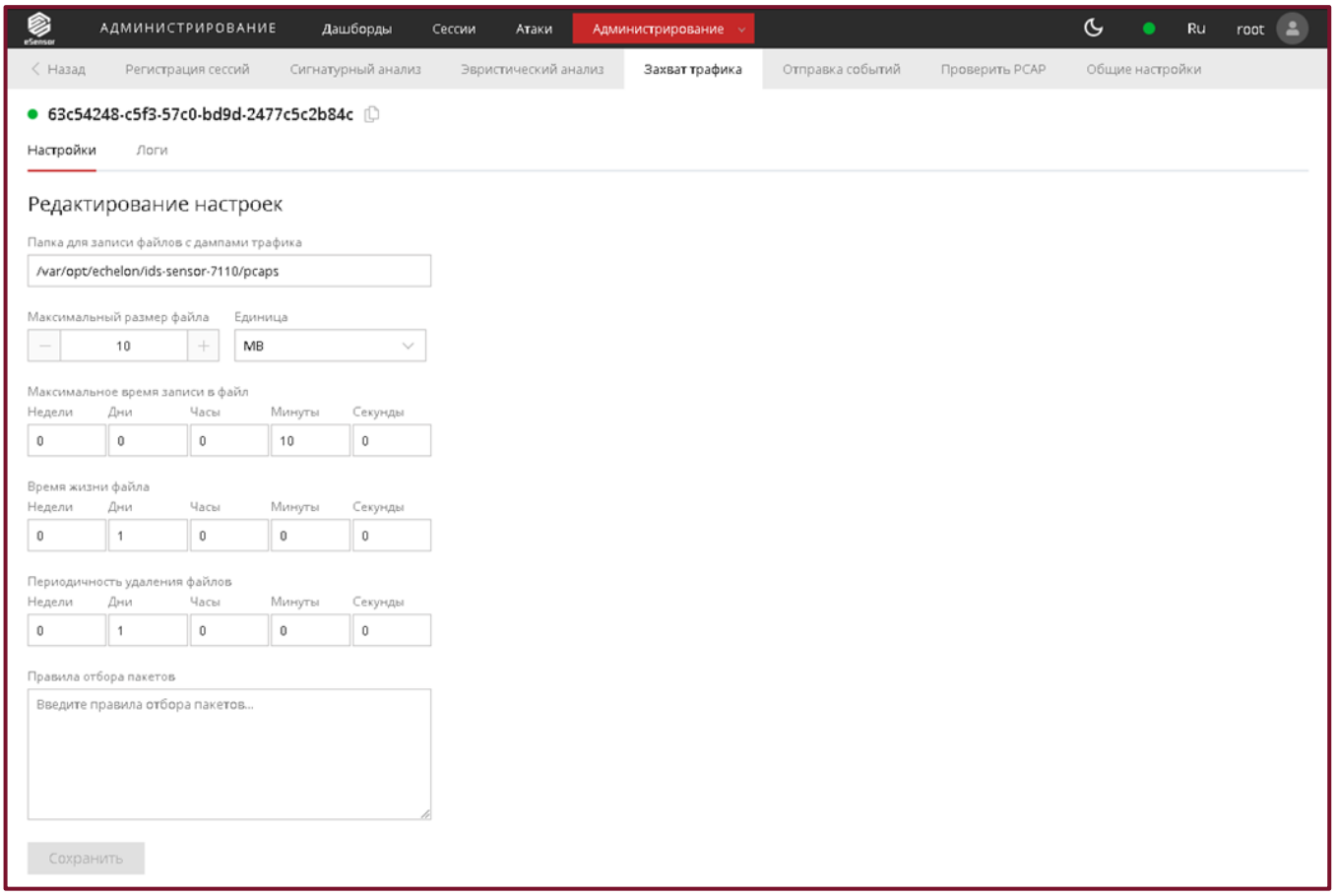

Рис. 45

Данное подменю карточки сенсора предназначено для просмотра настроек автоматического сохранения сетевого трафика в виде PCAP-файлов, заданных администратором eSensor. Подменю состоит из вкладок «Настройки» и «Логи».

Вкладка «Настройки» предназначена для настройки модуля захвата трафика сенсора, а вкладка «Логи» – для отображения системного журнала модуля захвата трафика сенсора eSensor.

Доступны следующие настройки:

– «Папка для записи файлов с дампами трафика» – путь в файловой системе машины с сенсором к папке, в которую необходимо записывать дампы трафика. Дампы записываются в файлы формата «PCAP»;

– «Максимальный размер файла» – максимальный размер PCAP-файла с записываемым трафиком, по достижении которого происходит ротация записи;

– «Максимальное время записи в файл» – максимальное время записи трафика в PCAP-файл, по достижении которого происходит ротация записи;

– «Время жизни файла» – время существования PCAP-файла, по прошествии которого он попадет в категорию для удаления при следующем удалении файлов;

– «Периодичность удаления файлов» – периодичность, с которой будет производиться удаление PCAP-файлов с превышенным временем жизни;

– «Правила отбора пакетов» – настройки BPF. Формат вводимых данных соответствует синтаксису BPF.

Для изменения настроек модуля необходимо:

1) перейти на вкладку «Настройки» страницы «Администрирование» → «Сенсоры» → «Сенсор» → «Захват трафика»;

2) изменить необходимые настройки;

3) нажать кнопку «Сохранить».

4.6.2.2.5. Подменю «Отправка событий»

Подменю «Отправка событий» карточки сенсора представлено на рис. 46.

Подменю «Отправка событий» карточки сенсора

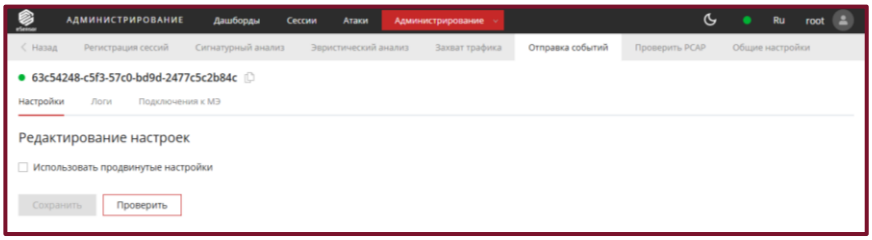

Рис. 46

Подменю «Отправка событий» карточки сенсора состоит из следующих функциональных вкладок:

– «Настройки» – данная вкладка предназначена для просмотра пользовательских настроек отправки регистрируемых сенсором событий ИБ в SIEM-системы;

– «Логи» – аналогично предыдущим подменю карточки сенсора, данная вкладка предназначена для просмотра системного журнала модуля отправки событий сенсора eSensor.

Настройка модуля

На вкладке «Настройки» страницы «Администрирование» → «Сенсоры» → «Сенсор» → «Отправка событий» предоставляет возможность задать настройки модуля отправки событий сенсора (рис. 47).

Активная настройка «Использовать продвинутые настройки» позволяет редактировать поле для задания настроек отправки событий ИБ в SIEM-системы.

Вкладка «Настройки» подменю «Отправка событий» карточки сенсора

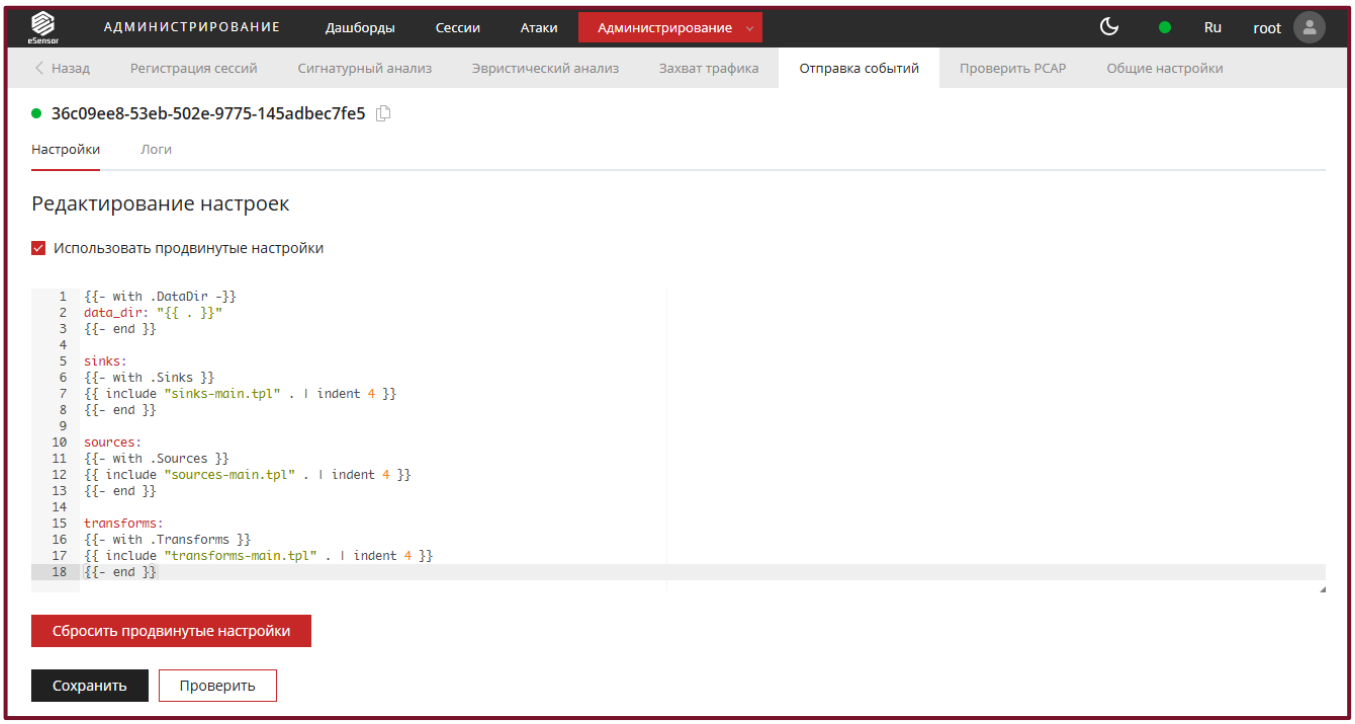

Рис. 47

4.6.2.2.6. Подменю «Проверить PCAP»

Подменю «Проверить PCAP» карточки сенсора представлено на рис. 48.

Подменю «Проверить PCAP» карточки сенсора

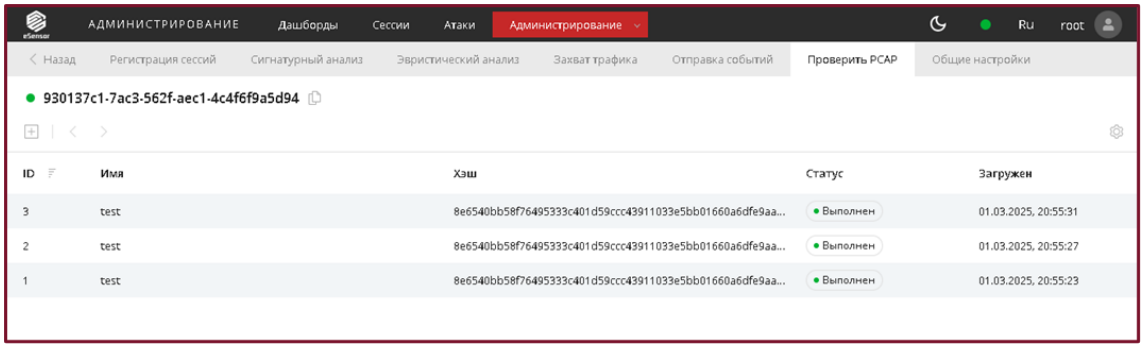

Рис. 48

Данное подменю карточки сенсора предназначено для проверки созданных в eSensor или загруженных с рабочей станции PCAP-файлов. При переходе к этому подменю карточки сенсора eSensor отображает таблицу, содержащую информацию о выполненных запросах проверки PCAP-файлов. В случае отсутствия завершенных запросов на проверку файлов в данном подменю отобразится пустая таблица и надпись «Нет данных».

В eSensor предусмотрена возможность выбрать, какие виды анализа трафика необходимо использовать при проверке PCAP-файла:

– регистрация сессий;
– сигнатурный анализ;
– эвристический анализ.

Примечание. Для проведения проверки PCAP-файла сетевого трафика, этот файл должен быть загружен в СУС eSensor. Сделать это можно на вкладке «Управление PCAP-файлами» меню «Администрирование».

Для добавления нового запроса на проверку PCAP-файла необходимо нажать на кнопку добавления « ⊞ » после чего отобразится окно добавления нового запроса проверки PCAP-файла (рис. 49).

Создание нового запроса проверки PCAP-файла

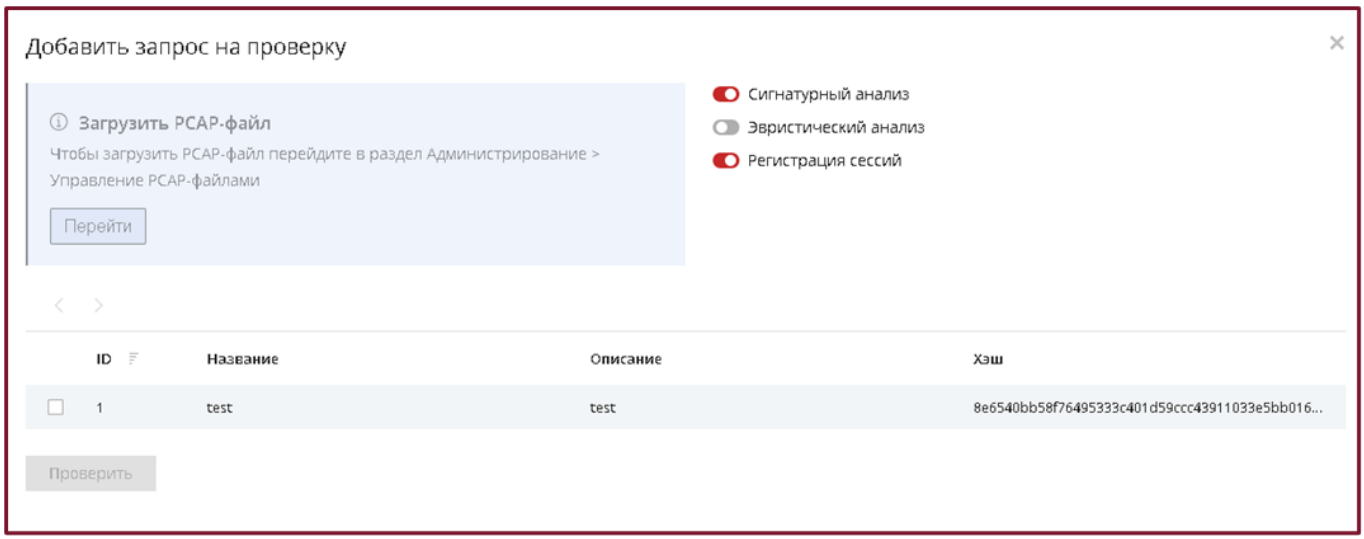

Рис. 49

В окне создания нового запроса проверки PCAP-файла необходимо выбрать применяемые опции (регистрация сессий, сигнатурный и эвристический анализ) и файл, для которого будет производится проверка. После чего нажать на кнопку «Проверить» слева внизу окна создания нового запроса проверки файла сетевого трафика. Для выхода из данного окна необходимо нажать на крестик в правом верхнем углу.

После нажатия на кнопку «Проверить» новый запрос проверки файла сетевого трафика отобразится в таблице запросов. В eSensor предусмотрена возможность просмотра подробных данных о выполненных проверках PCAP-файлов в карточке запроса на проверку файла. Для перехода к такой карточке необходимо нажать в любом месте на строку таблицы, соответствующей интересующему PCAP-файлу. После чего отобразится карточка запроса на проверку файла, представленная на рис. 50.

Карточка запроса на проверку файла

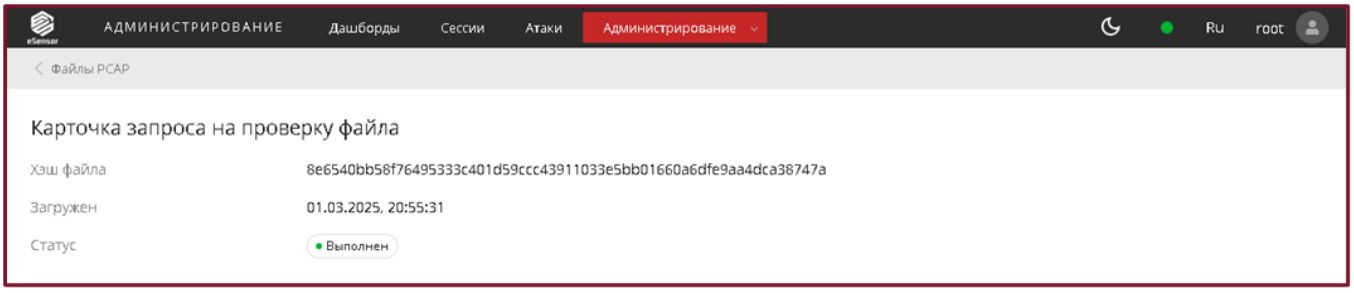

Рис. 50

В карточке запроса на проверку файла отображается следующая информация:

– «Хэш файла» – хэш-сумма проверяемого PCAP-файла;

– «Загружен» – дата и время загрузки файла на проверку (создания данного запроса);

– «Статус» – статус запроса («Выполнен», «Выполняется», «Отменен», «Ошибка»).

4.6.2.2.7. Подменю «Общие настройки»

Подменю «Общие настройки» карточки сенсора представлено на рис. 51.

Подменю «Общие настройки» карточки сенсора

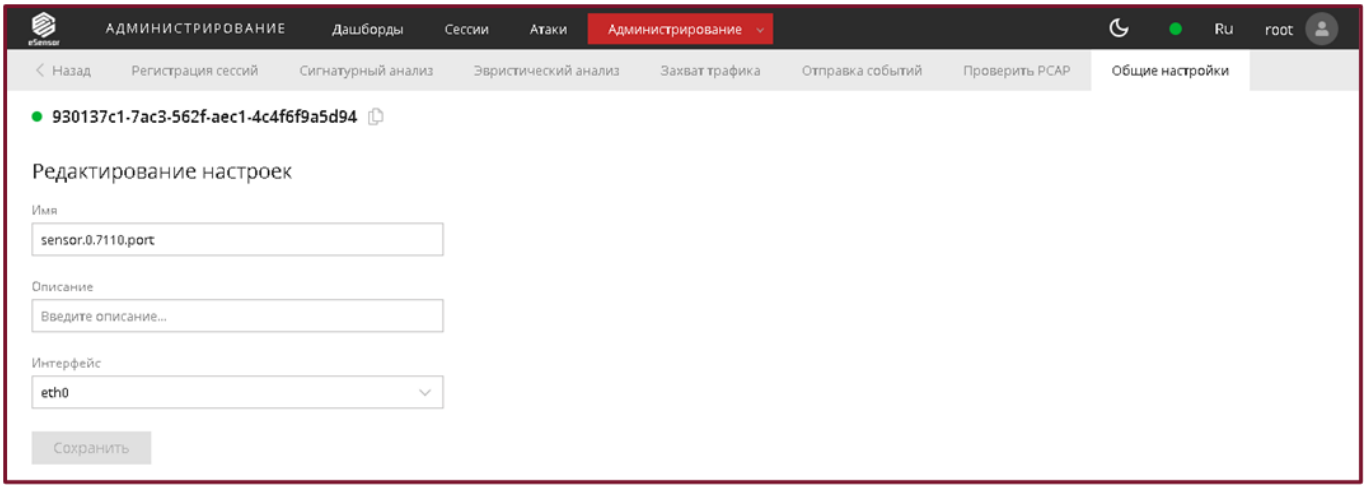

Рис. 51

Данное подменю карточки сенсора для оператора eSensor с ролью **«Пользователь»** носит **исключительно информационный характер** и содержит такую информацию непосредственно о сенсоре, как:

– «Имя» – наименование сенсора, задаваемое администратором eSensor при регистрации нового сенсора в системе;

– «Описание» – дополнительная информация о сенсоре, которую администратор eSensor посчитал необходимым указать при регистрации данного сенсора в системе;

– «Интерфейс» – интерфейс машины с сенсором, трафик которого должен захватывать и анализировать сенсор.

4.6.2.3. Подключение сенсоров

Для подключения установленного сенсора к СУС необходимо:

1) перейти на страницу «Администрирование» → «Сенсоры»;

2) нажать кнопку « ⊞ ». Откроется страница добавления сенсора (рис. 52);

Страница добавления сенсора

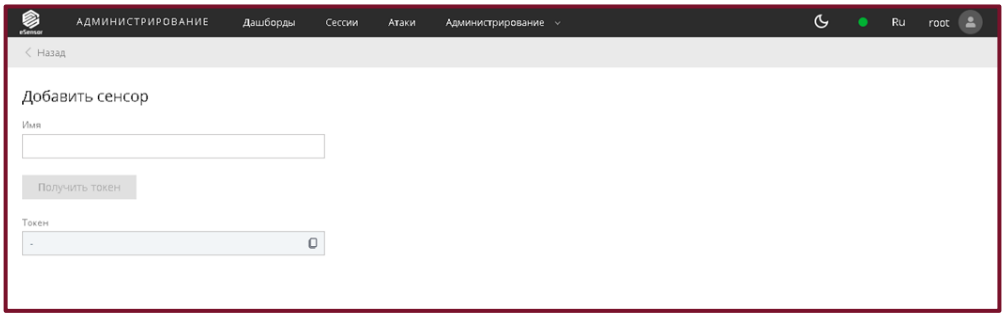

Рис. 52

3) ввести в поле «Имя» наименование, которое необходимо назначить подключаемому сенсору;

4) нажать кнопку «Получить токен». В поле «Токен» сгенерируется токен;

5) скопировать токен из поля «Токен»;

6) подключиться к локальной консоли управления машины, на которой установлен сенсор, который необходимо подключить к СУС;

7) остановить службу сенсор, который необходимо подключить к СУС, передав следующую команду:

`sudo systemctl stop ids-sensor@<Порт>`, где <Порт> – порт, по которому по умолчанию доступен сенсор;

8) запустить сенсор в режиме регистрации, передав команду:

`sudo /opt/echelon/ids-sensor/ids-sensor register -c /opt/echelon/ids-sensor-<Порт>/config.yaml --token <Токен> --server-addr <Адрес_СУС>:<Порт_СУС>`, где:

а) `<Порт>` – порт, по которому по умолчанию доступен сенсор;

б) `<Токен>` – токен, скопированный на подпункте 5);

в) `<Адрес_СУС>` – адрес (доменное имя), на которое выписан TLS-сертификат СУС (по умолчанию данный сертификат выписывается на доменное имя, заданное при установке в файле `hosts_esensor.yml` в качестве значения ключа `all.children.esensor_backend.hosts`);

г) `<Порт_СУС>` – порт, по которому доступен СУС (по умолчанию – 7100).

Регистрация сенсора пройдена успешна, если в процессе выполнения команды в локальной консоли управления не было выведено сообщений об ошибках (сообщения с пометками `WARN` и `DEBUG`, генерируемые в процессе выполнения команды, являются информационными и не являются сообщениями об ошибках);

9) запустить службу зарегистрированного сенсора:

`sudo systemctl start ids-sensor@<Порт>`, где `<Порт>` – порт, по которому по умолчанию доступен сенсор;

10) проверить, что служба зарегистрированного сенсора работает, т.е. находится в статусе `active(running)`:

`sudo systemctl status ids-sensor@<Порт>`, где `<Порт>` – порт, по которому по умолчанию доступен сенсор.

Через некоторое время в таблице на странице «Администрирование» → «Сенсоры» должна появиться информация о подключенном сенсоре.

4.6.2.4. Отключение сенсоров

Для отключения сенсора необходимо:

1) выбрать сенсор, который необходимо отключить, выставив «☑» в строке с информацией о данном сенсоре в таблице сенсоров;

2) нажать кнопку « 🗑 ».

4.6.3. Вкладка «Управление PCAP-файлами»

4.6.3.1. Общая информация

Данная вкладка предназначена для работы с хранящимися на СУС eSensor PCAP-файлами сетевого трафика. Вкладка «Управление PCAP-файлами» представляет собой таблицу, содержащую информацию обо всех PCAP-файлах в хранилище (рис. 53).

Вкладка «Управление PCAP-файлами»

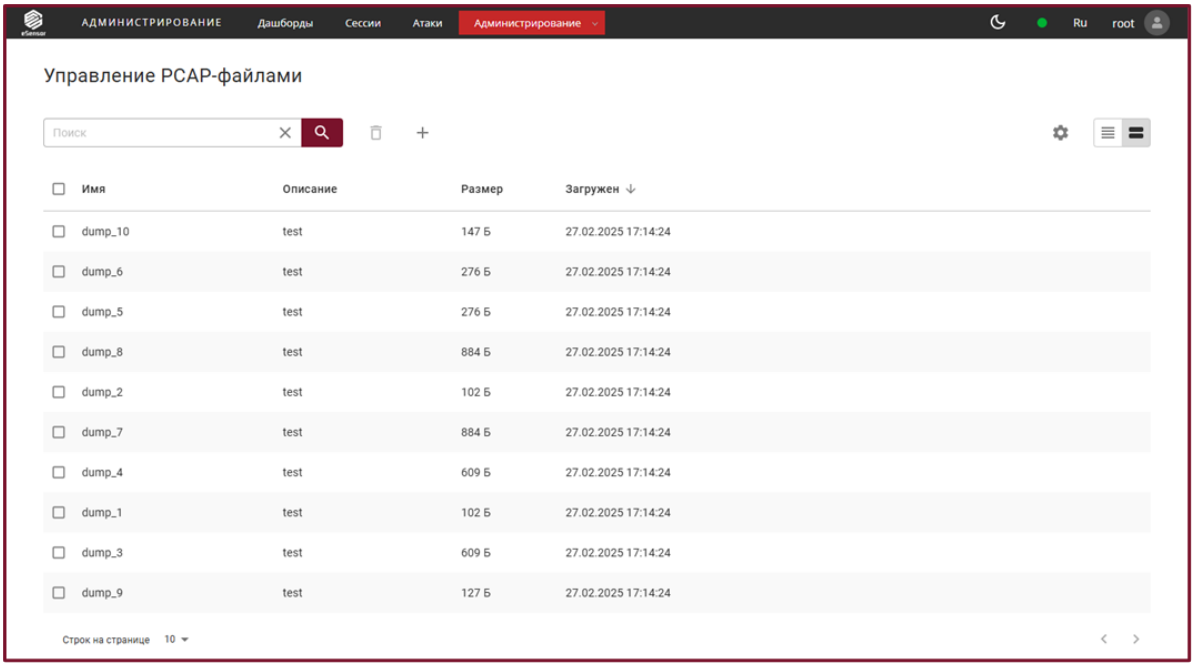

Рис. 53

Данная вкладка позволяет сделать следующее:

– просматривать таблицу PCAP-файлов, хранящихся на СУС;

– настраивать таблицу PCAP-файлов, хранящихся на СУС;

– загружать PCAP-файлы для хранения на СУС;

– просматривать и редактировать карточки загруженных PCAP-файлов, содержащих подробную информацию о файлах;

– удалять PCAP-файлы.

4.6.3.2. Загрузка PCAP-файлов

Для загрузки PCAP-файла с компьютера пользователя необходимо нажать на кнопку «Импортировать»; заполнить форму (рис. 54); нажать кнопку «Загрузить с компьютера» и выбрать файл, который требуется загрузить. Далее нажать кнопку «Загрузить».

Форма загрузки PCAP-файла

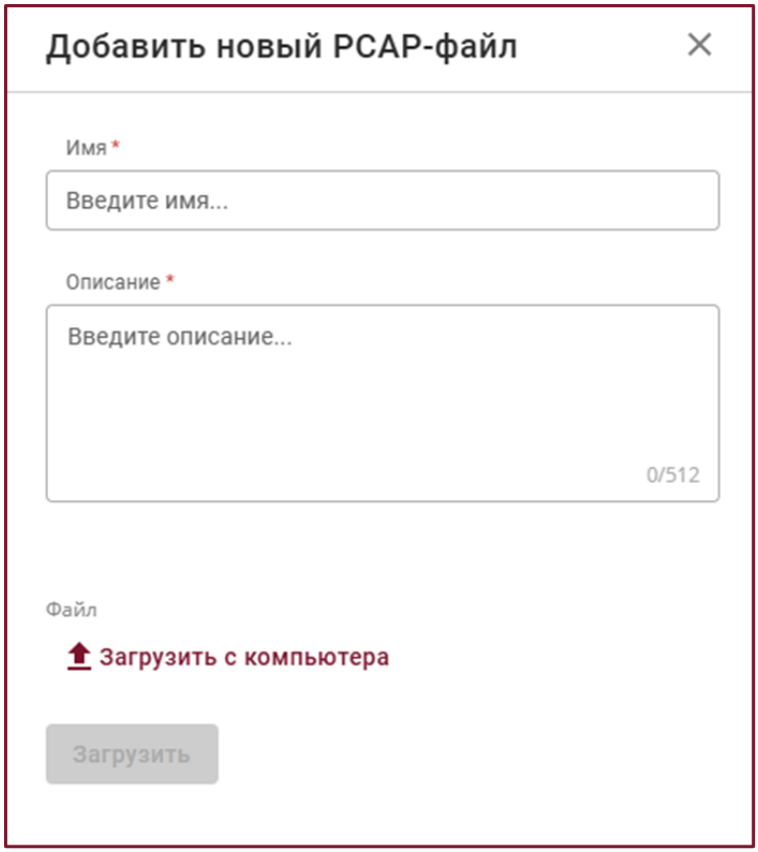

Рис. 54

4.6.3.3. Просмотр и редактирование карточки PCAP-файла

Для перехода к карточке PCAP-файла необходимо нажать на строку с информацией об интересуемом PCAP-файле таблицы PCAP-файлов. Откроется карточка выбранного PCAP-файла (рис. 55).

При нажатии кнопки «Скачать PCAP-файл» начнется скачивание файла.

Карточка PCAP-файла

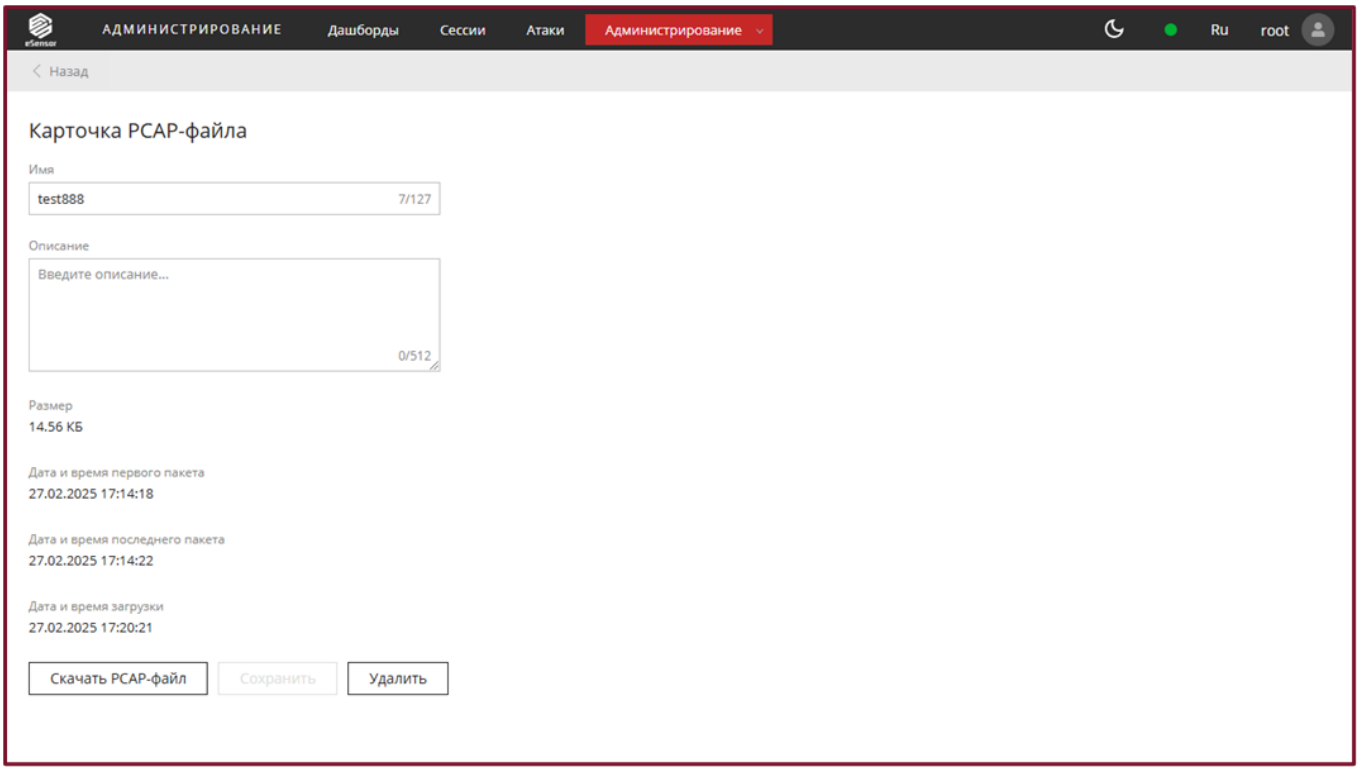

Рис. 55

4.6.3.4. Удаление PCAP-файлов из хранилища

Для удаления PCAP-файла из хранилища необходимо выбрать PCAP-файл, который требуется удалить, выставив «☑» в строке с информацией о данном файле таблицы PCAP-файлов, нажать кнопку « 🗑 ».

4.6.4. Вкладка «Запросы на копирование»

Вкладка «Запросы на копирование» предназначена для работы с запросами на копирование дампов сетевого трафика с сенсоров в хранилище на СУС: дампов сессий (п. 4.4.3 настоящего документа), а также дампов за выбранный период времени.

Данная вкладка представляет собой таблицу, содержащую информацию обо всех созданных запросах на копирование (рис. 56).

Вкладка «Запросы на копирование»

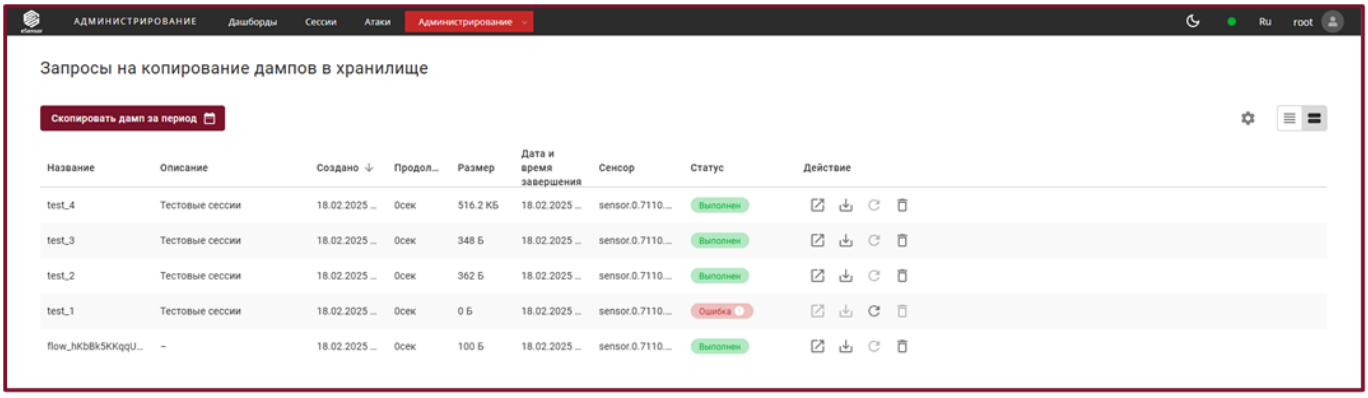

Рис. 56

Кнопка «Скопировать дамп за период» позволяет создать запрос на копирование в хранилище дампа трафика за выбранный период времени.

Примечание. Для возможности выгрузки трафика за период необходимо, чтобы на сенсоре были дампы трафика за этот период, записанные модулем захвата трафика сенсора. Инструкция по настройке данного модуля приведена в подразделе «Настройка записи сетевого трафика за период времени» документа «Система анализа сетевого трафика для обнаружения кибератак eSensor. Руководство администратора» НПЕШ.00404-01 91.

ВНИМАНИЕ!

Для выгрузки трафика за период выбранный период времени с сенсора в хранилище модуль «Захвата трафика» сенсора должен быть включен. При этом, при выполнении запроса выгрузится только тот трафик, который был зарегистрирован **на текущем назначенном сенсору сетевом интерфейсе**.

Если в хранилище еще нет копируемого дампа трафика, то при успешном выполнении запроса в хранилище на СУС (п. 4.6.3 настоящего документа) будет создана копия этого дампа. Если такой дамп уже есть (полное совпадение содержимого), новая копия создана не будет, запрос будет ссылаться на существующую копию.

Если дампа нет на сенсоре, например, он уже был полностью удален с сенсора при ротации, запрос завершится со статусом «Ошибка».

4.6.5. Вкладка «Группы правил»

4.6.5.1. Общая информация

Для работы с решающими правилами в eSensor используется механизм групп правил. Группа правил – это объединение множества правил, полученных из одного источника. Правила можно загружать в группу из источника правил, загружать из архива или создавать непосредственно в самой группе. Источником правил может быть удаленный Git-репозиторий, FTP- или SMB-сервер или другая группа правил. Группы правил хранятся на СУС и загружаются на выбранные сенсоры.

На вкладке «Группы правил» осуществляется управление группами правил (рис. 57).

Вкладка «Группы правил»

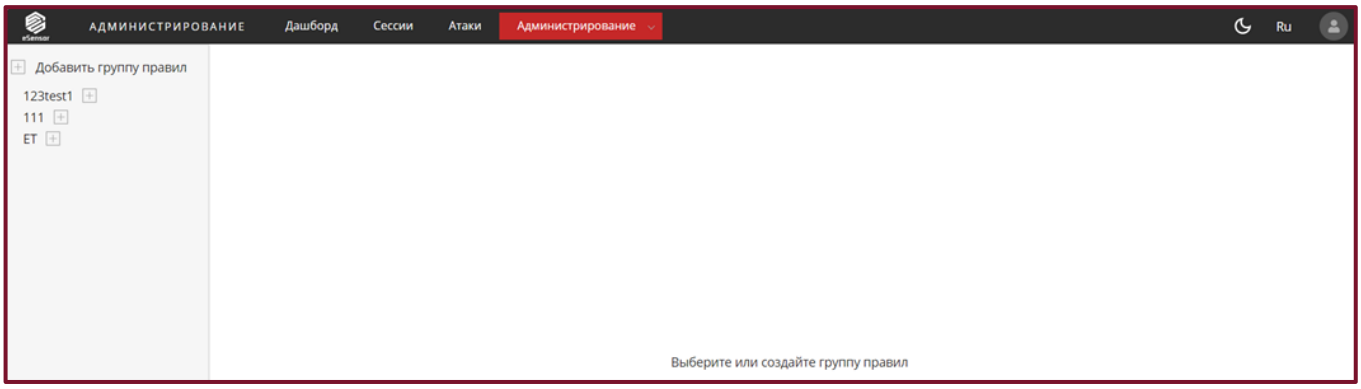

Рис. 57

Данная вкладка позволяет:

– просматривать список групп правил;

– добавлять группы правил;

– управлять конкретной группой правил.

В левой части вкладки отображается список добавленных групп правил (рис. 58).

Список групп правил

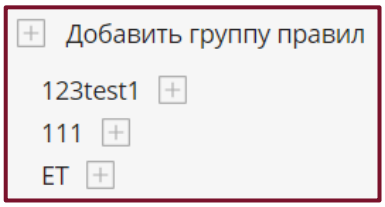

Рис. 58

При нажатии на имя конкретной группы в списке групп правил в правой части страницы появится интерфейс управления выбранной группой (рис. 59).

Интерфейс управления группой правил

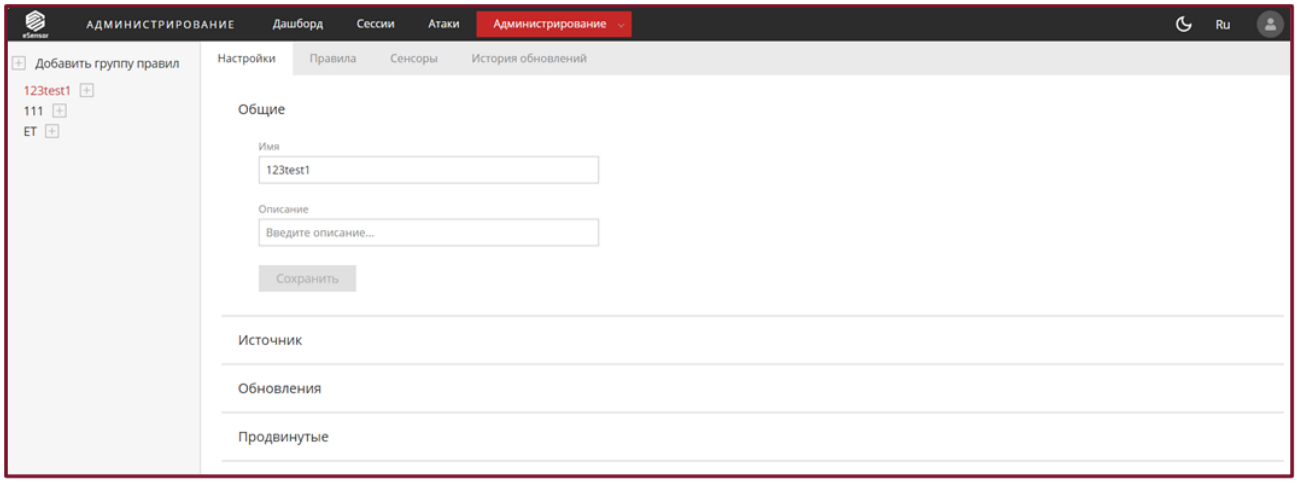

Рис. 59

Данный интерфейс состоит из следующих вкладок:

– «Настройки» – на которой можно задать настройки группы;

– «Правила» – на которой можно управлять правилами группы;

– «Сенсоры» – на которой можно управлять сенсорами, использующими группу;

– «История обновлений» – на которой можно управлять обновлениями группы.

4.6.5.2. Добавление группы правил

Для добавления группы правил необходимо выполнить следующее:

1) нажать « ⊞ Добавить группу правил»;

2) заполнить появившуюся форму. Состав полей формы зависит от выбранного значения поля «Тип» (см. рис. 60);

3) нажать кнопку «Сохранить».

Интерфейс добавления группы правил

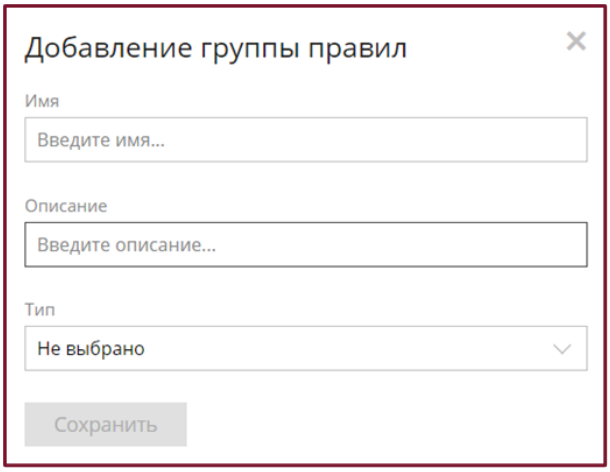

Рис. 60

Форма добавления группы правил содержит поля, описание которых представлено в таблице 7.

Таблица 7 – Поля формы добавления группы правил

Поле	Описание и возможные значения	Пример
Имя	Имя группы. Обязательное поле	suricata rules
Описание	Произвольное текстовое описание	Правила из Gitea
Тип	Тип группы, определяющий способ загрузки правил. Обязательное поле. Возможные значения: – «Не выбрано»; – «Git»; – «FTP»; – «SMB»; – «Другая группа»	Git

При выборе типа «Не выбрано» создаётся пустая группа правил. Источник правил при этом отсутствует.

При выборе типа «Git» источником группы правил будут являться файлы «.rules» с правилами, хранящиеся в репозитории на удаленном сервере Git. При этом форма добавления группы правил примет следующий вид (рис. 61).

Добавление группы правил через Git

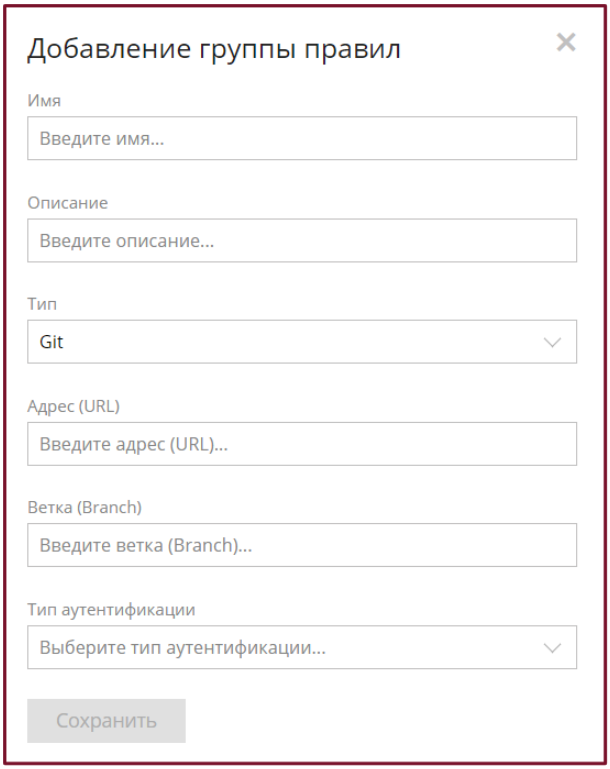

Рис. 61

В форме появятся дополнительных поля, представленные в таблице 8.

Таблица 8 – Дополнительные поля формы добавления группы правил через Git

Поле	**Описание и возможные значения**	**Пример**
Адрес (URL)	Адрес удаленного git-репозитория, в котором хранятся файлы с правилами «.rules». Обязательное поле	http://192.168.0.1:3000/ gitea/rules_repo
Ветка (Branch)	Ветка git-репозитория, содержащая файлы с правилами. Обязательное поле	master
Тип аутентификации	Тип аутентификации на сервере Git. Обязательное поле. Возможные значения: – «Без аутентификации»; – «Логин-пароль»; – «По токену»	Без аутентификации

При выборе типа «FTP» источником группы правил будут являться файлы «.rules» с правилами, хранящиеся на удаленном FTP-сервере. При этом форма добавления группы правил примет следующий вид (рис. 62).

Форма добавления группы правил через FTP

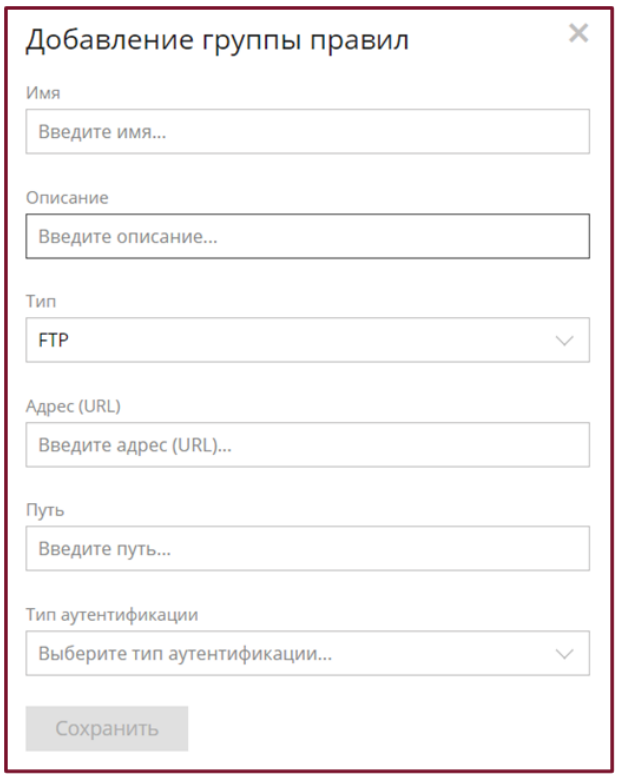

Рис. 62

В форме появятся дополнительных поля, представленные в таблице 9.

Таблица 9 – Дополнительные поля формы добавления группы правил через FTP

Поле	**Описание и возможные значения**	**Пример**
Адрес (URL)	Адрес удаленного компьютера, на котором хранятся файлы с правилами. Обязательное поле	192.168.0.1
Путь	Путь к каталогу с файлами с правилами на FTP-сервере (относительно корневого каталога FTP-сервера). Обязательное поле	rules/open
Тип аутентификации	Тип аутентификации на FTP-сервере. Обязательное поле. Возможные значения: – «Без аутентификации»; – «Логин-пароль»; – «По токену»	Логин-пароль

При выборе типа «SMB» источником группы правил будут являться файлы «.rules» с правилами, хранящиеся на удаленном компьютере и загружаемые в eSensor по протоколу SMB. При этом форма добавления группы правил примет следующий вид (рис. 63).

Форма добавления группы правил через SMB

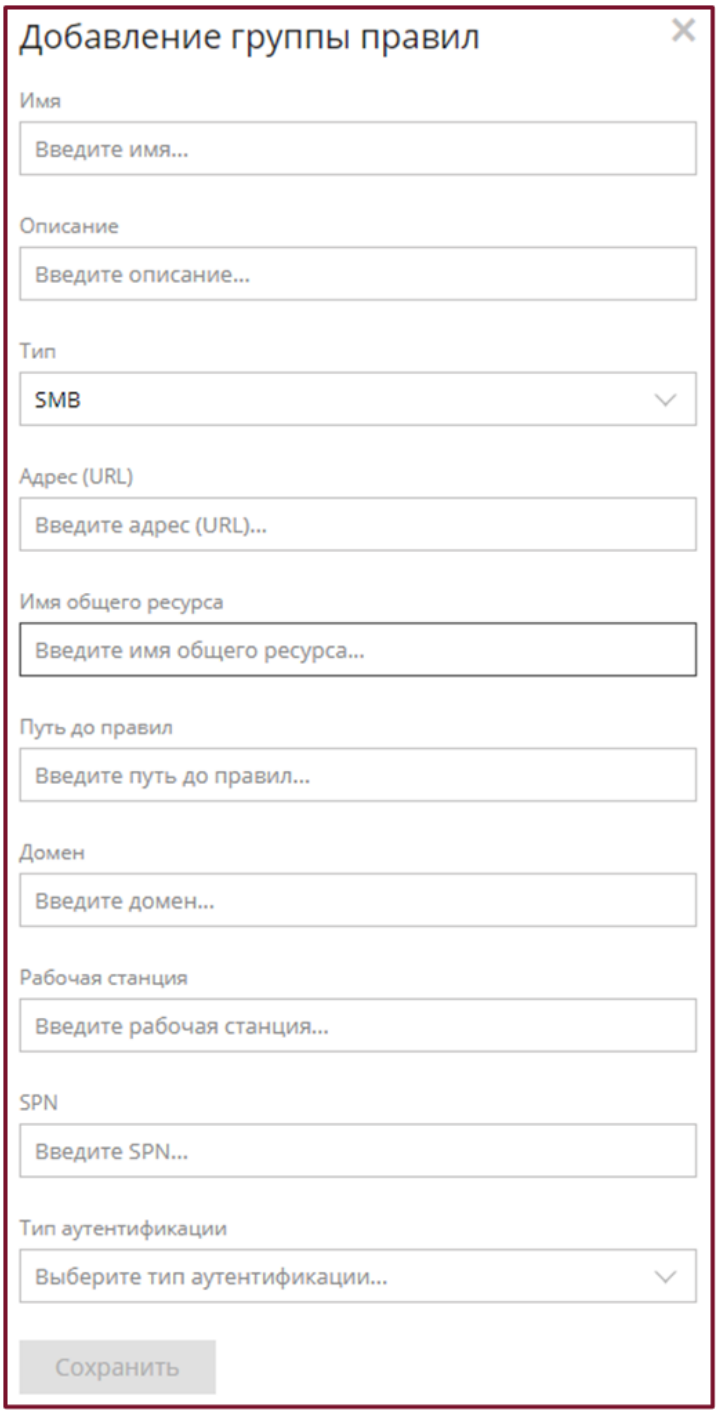

Рис. 63

В форме появятся дополнительных поля, представленные в таблице 10.

Таблица 10 – Дополнительные поля формы добавления группы правил через SMB

Поле	Описание и возможные значения	Пример
Адрес (URL)	Адрес удаленного компьютера с файлами с правилами. Обязательное поле	192.168.0.1
Имя общего ресурса	Название общего ресурса SMB-сервера. Обязательное поле	public
Путь до правил	Путь к каталогу с правилами относительно общего ресурса. Обязательное поле	rules (прим.: это соответствует public/rules)
Домен	Домен	WORKGROUP
Рабочая станция	Рабочая станция	HOME-PC
SPN	SPN. Формат: service/hostname[:port]	cifs/remotehost:1020

При выборе типа «Другая группа» источником группы правил будет являться другая группа правил. При добавлении таким способом возникает следующая иерархия между группами: добавляемая группа является дочерней по отношению к группе, на основе которой она создается. Это означает следующее:

– при создании дочерняя группа наследует все правила родительской группы;

– обновления правил в родительской группе также происходят и в дочерней группе.

При выборе типа «Другая группа» форма добавления группы правил примет вид, который представлен на рис. 64.

Форма добавления группы правил на основе другой группы

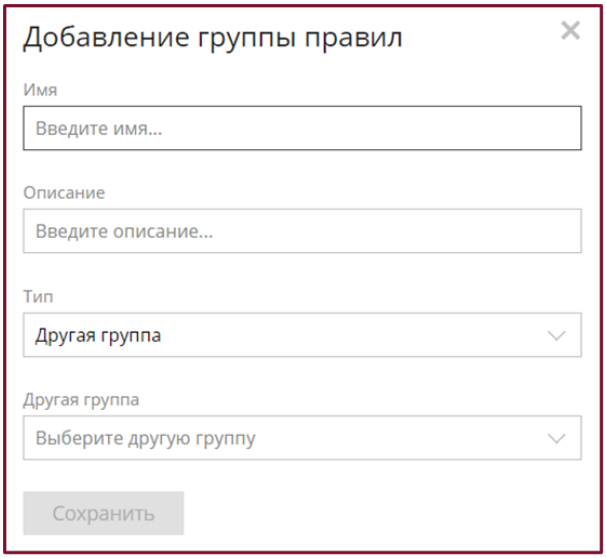

Рис. 64

В форме появятся дополнительных поля, представленные в таблице 11.

Таблица 11 – Дополнительные поля формы добавления группы правил при выборе типа «Другая группа»

Поле	Описание и возможные значения	Пример
Другая группа	Имя родительской группы. Значение выпадающего списка, состоящего из имен добавленных ранее групп. Обязательное поле	parent group

При загрузке правил через Git, FTP и SMB необходимо выбрать один из доступных способов аутентификации на сервере источника:

– «Без аутентификации»;

– «Логин-пароль»;

– «По токену».

При выборе типа аутентификации «Без аутентификации» подключение к серверу источника правил будет произведено без аутентификации.

При выборе типа аутентификации «Логин-пароль» в соответствующих полях необходимо указать учетные данные пользователя сервера с источником правил, имеющего права на скачивание файлов (рис. 65).

Аутентификация по логину и паролю

Рис. 65

Описание полей «Логин» и «Пароль» приведено в таблице 12.

Таблица 12 – Описание полей «Логин» и «Пароль»

Поле	Описание и возможные значения	Пример
Логин	Логин. Обязательное поле	login
Пароль	Пароль. Обязательное поле	password

При выборе типа аутентификации «По токену» необходимо указать токен в соответствующем поле (рис. 66).

Аутентификация по токену

Рис. 66

Описание поля «Токен» приведено в таблице 13.

Таблица 13 – Описание поля «Токен»

Поле	Описание и возможные значения	Пример
Токен	Токен для аутентификации. Обязательное поле	21S71D8Hdh181dgada

После добавления группы, если для нее был указан источник, начнется загрузка правил из данного источника. Статус и другую информацию о загрузке (обновлении) можно просмотреть на вкладке «История обновлений» (п. 4.6.5.6 настоящего документа).

При необходимости можно настроить расписание автоматических обновлений группы (п. 4.6.5.3 настоящего документа).

4.6.5.3. Настройка группы правил

Настройка группы правил осуществляется на вкладке «Настройки» страницы «Администрирование» → «Группы правил» → «Группа правил» (рис. 67).

Вкладка «Настройки» страницы «Группа правил»

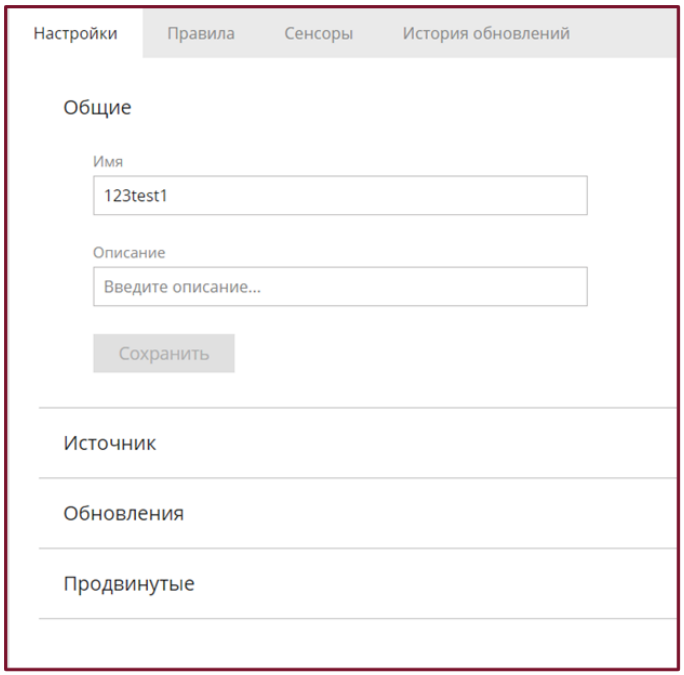

Рис. 67

Данная вкладка содержит следующие блоки настроек группы правил:

– «Общие»;

– «Источник»;

– «Обновления»;

– «Продвинутые».

В блоке «Общие» расположена настройка имени группы правил (рис. 68).

Блок «Общие»

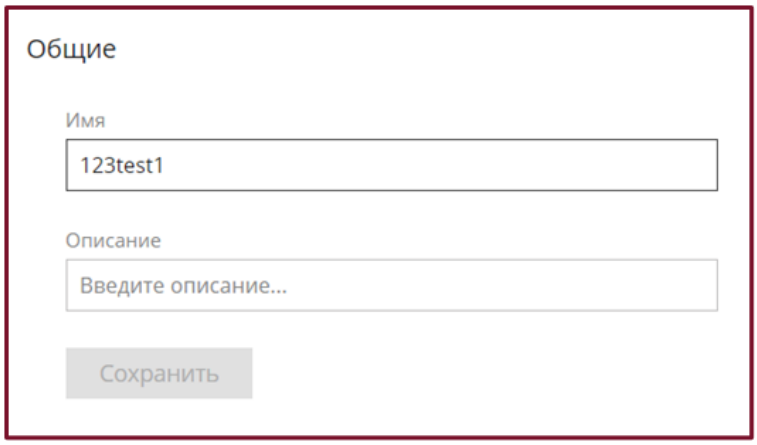

Рис. 68

В блоке «Источник» расположены настройки загрузки правил из источника правил (рис. 69).

Блок «Источник»

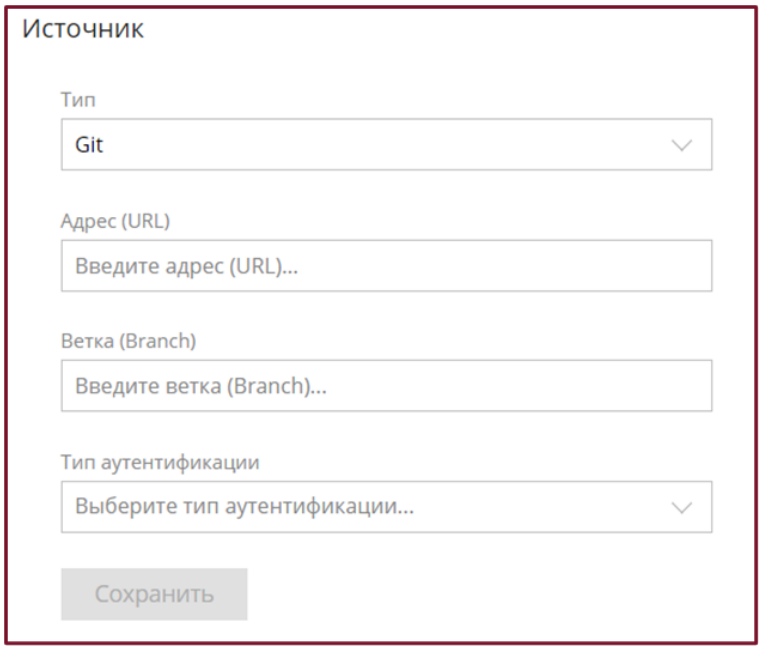

Рис. 69

В блоке «Обновления» расположены настройки обновлений группы правил (рис. 70).

Блок «Обновления»

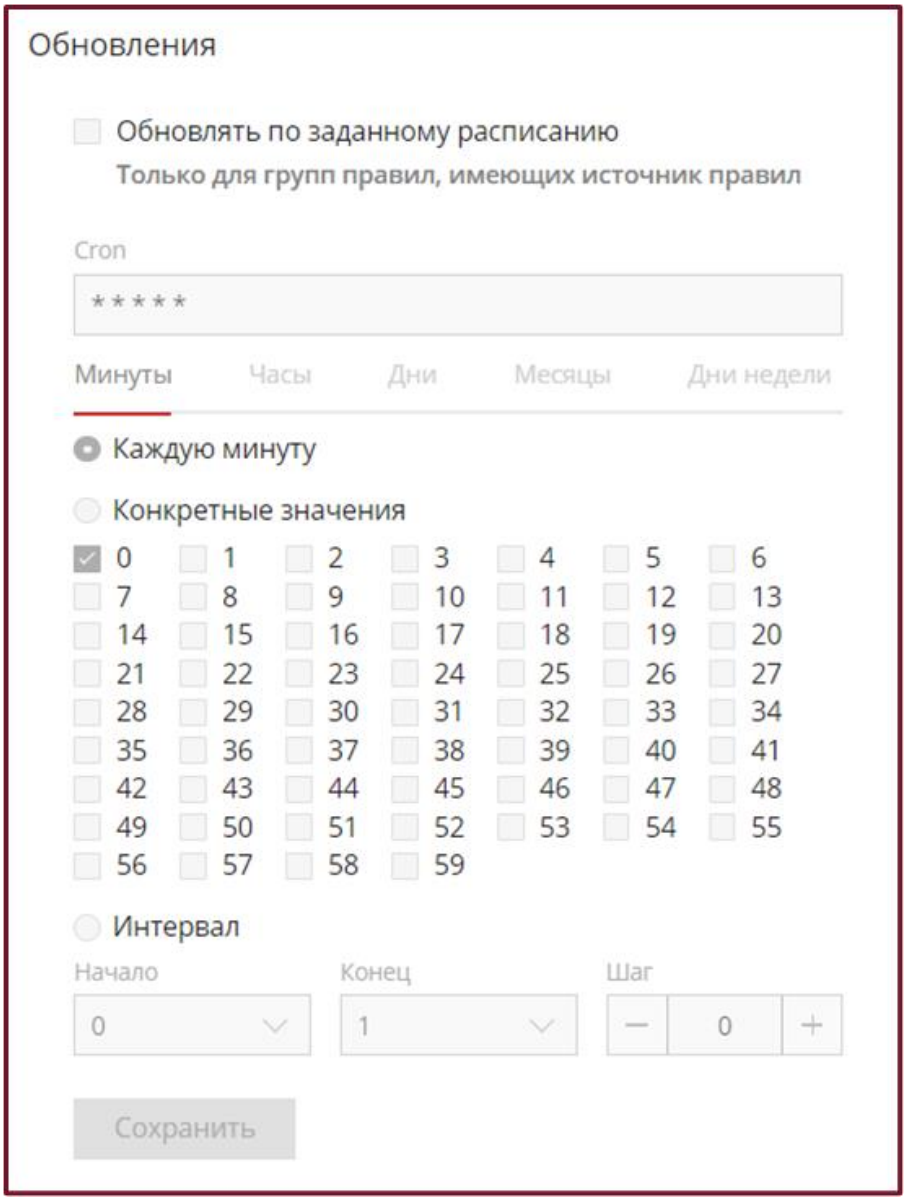

Рис. 70

В данном блоке присутствуют следующие настройки:

– чек-бокс «Обновлять по заданному расписанию» (активирование доступно только для групп правил, имеющих источник правил);

– настройки поля «Cron» для задания расписания.

Если группа правил имеет родительскую группу, то кроме перечисленных выше настроек в данной секции будет еще одна – «Обновлять автоматически с родительской группой правил» (рис. 71).

Настройка «Обновлять автоматически с родительской группой правил»

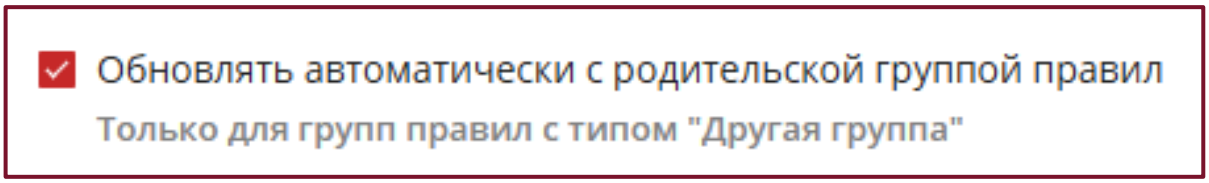

Рис. 71

ВАЖНО:

– рекомендуется настроить расписания обновлений созданных групп правил таким образом, чтобы все группы обновлялись **в разное время**;

– рекомендуется настроить расписание так, чтобы группы правил обновлялись тогда, когда **меньше всего сетевая активность** (обычно ночью);

– **не рекомендуется настраивать слишком частые обновления**, например, каждую минуту. Минимальный рекомендуемый интервал обновлений – раз в час.

В блоке «Продвинутые» находится кнопка удаления группы правил (рис. 72).

Блок «Продвинутые»

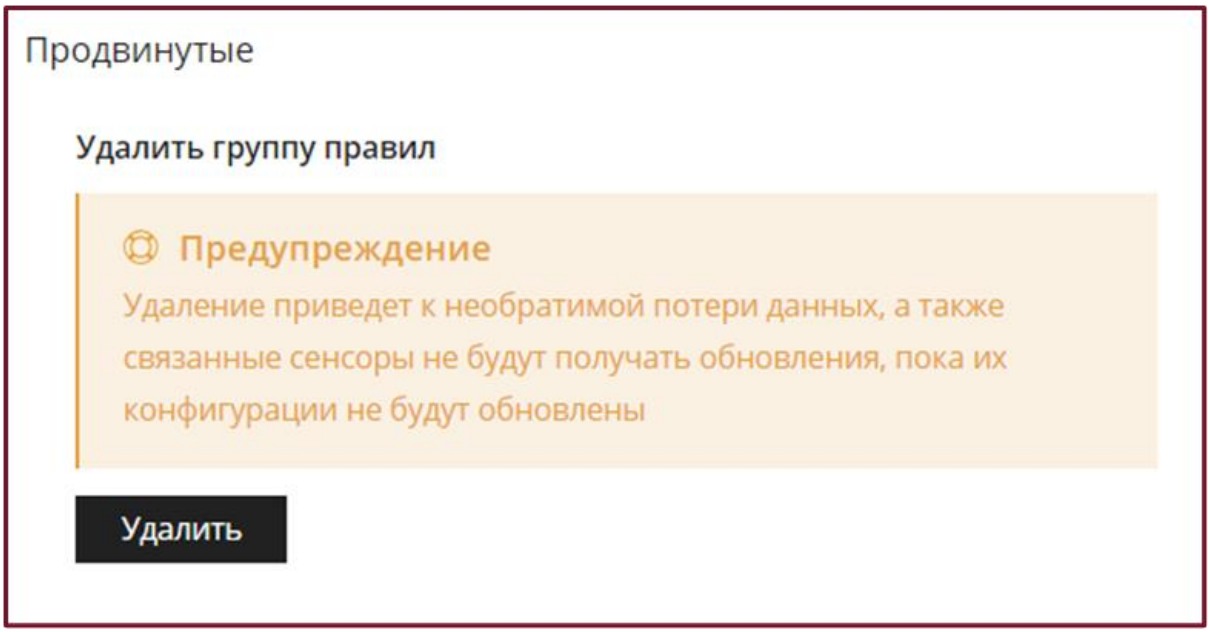

Рис. 72

Перед удалением группы необходимо удостовериться, что ее не использует ни один сенсор (т.е. таблица сенсоров на вкладке «Сенсоры» пуста).

4.6.5.4. Управление правилами группы

4.6.5.4.1. Общая информация

Управление правилами группы осуществляется на вкладке «Правила» страницы «Администрирование» → «Группы правил» → «Группа правил» (рис. 73).

Вкладка «Правила» страницы «Группа правил»

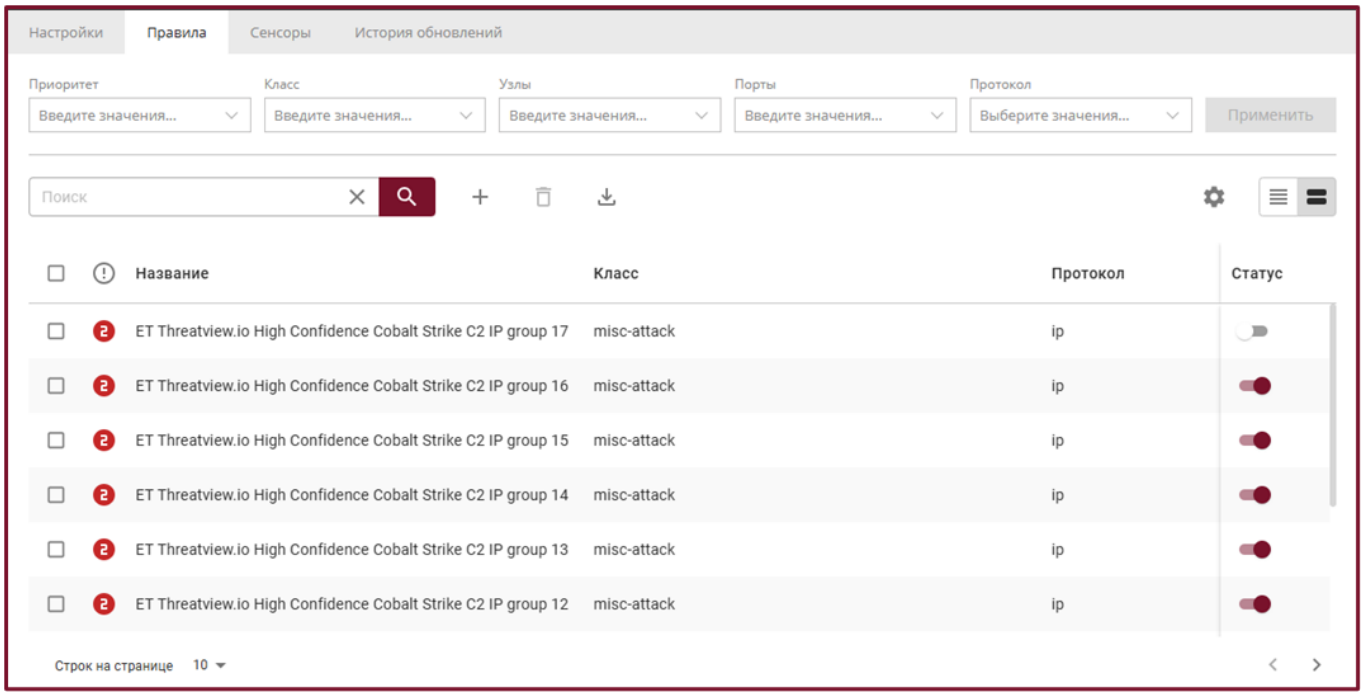

Рис. 73

Данная вкладка предоставляет возможность:

– просматривать таблицу правил группы;

– настраивать таблицу правил группы;

– загружать правила из архива;

– добавлять правила в группу (через редактор правил);

– переходить к карточке конкретного правила, для просмотра подробной информации о нем и редактирования;

– включать/выключать правила;

– удалять правила из группы.

ВНИМАНИЕ!

Чтобы изменения в правилах вступили в силу на сенсорах, использующих данную группу правил, необходимо обновить правила на данных сенсорах (п. 4.6.5.5.3 настоящего документа).

4.6.5.4.2. Загрузка правил из архива

Для загрузки правил в группу правил из архива необходимо:

1) нажать на иконку « ⬇ », откроется форма загрузки архива в группу правил (рис. 74);

Форма загрузки архива

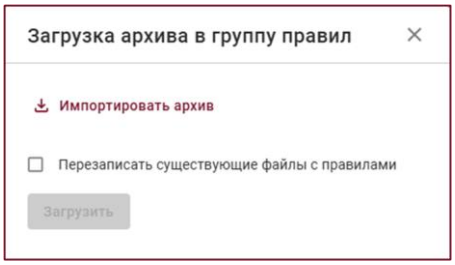

Рис. 74

2) нажать на кнопку « ⬇ Импортировать архив» и выбрать архив для загрузки. Архив должен иметь расширение «.zip», «.tar.gz» или «.tgz»;

3) если в группе правил уже есть файлы с правилами и требуется перезаписать их содержимое, активировать опцию «Перезаписать существующие файлы с правилами»;

4) нажать кнопку «Загрузить».

При успешной загрузке архива на экране появится окно (рис. 75) и начнется процесс проверки загружаемых правил. Статус и другую информацию о проверке (обновлении) можно просмотреть на вкладке «История обновлений» (п. 4.6.5.6 настоящего документа).

Успешная загрузка архива

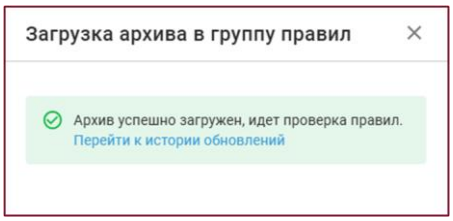

Рис. 75

ВНИМАНИЕ!

Чтобы изменения в правилах вступили в силу на сенсорах, использующих данную группу правил, необходимо обновить правила на данных сенсорах (п. 4.6.5.5.3 настоящего документа).

4.6.5.4.3. Добавление правил

Для добавления нового правила в группу правил необходимо нажать на кнопку « ⊞ », заполнить появившуюся форму (рис. 76) и нажать на кнопку «Сохранить» внизу страницы.

Форма добавления нового правила

Рис. 76

Описание полей формы добавления нового правила приведено в таблице 14.

Таблица 14 – Описание полей формы добавления нового правила

Поле	Описание и возможные значения	Пример
Файл	Название файла с расширением «.rules», в который нужно сохранить правило. Обязательное поле	dir1/dir2/test.rules

Поле	Описание и возможные значения	Пример
Правило	Выражение, написанное с соблюдением синтаксиса решающих правил. Обязательное поле	alert tcp any any -> any 502 (msg:"SURICATA TCP port 502 but not MODBUS"; flow:to_server; app-layer-protocol:!modbus; sid:2271018; rev:1;)

ВНИМАНИЕ!

Чтобы изменения в правилах вступили в силу на сенсорах, использующих данную группу правил, необходимо обновить правила на данных сенсорах (п. 4.6.5.5.3 настоящего документа).

4.6.5.4.4. Редактирование правил

Для редактирования правила необходимо кликнуть по строке с правилом, которое необходимо редактировать. Откроется страница редактирования данного правила (рис. 77). Далее необходимо внести нужные правки и нажать «Сохранить».

Страница редактирования правила

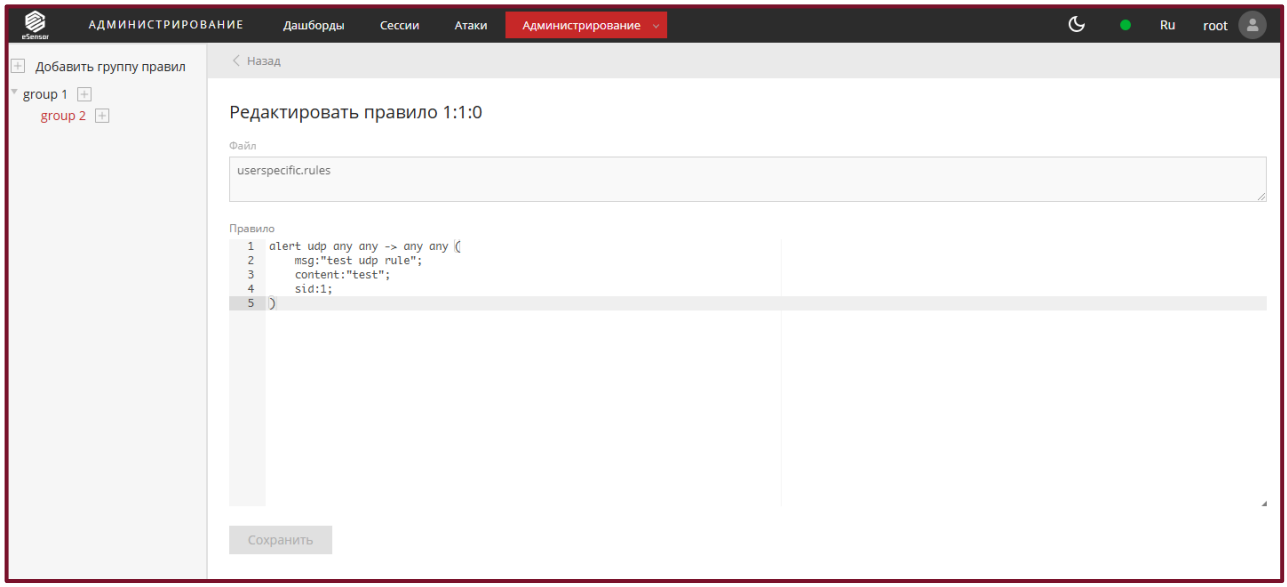

Рис. 77

ВНИМАНИЕ!

Чтобы изменения в правилах вступили в силу на сенсорах, использующих данную группу правил, необходимо обновить правила на данных сенсорах (п. 4.6.5.5.3 настоящего документа).

4.6.5.4.5. Включение и выключение правил

Для включения/выключения правила необходимо установить переключатель столбца «Статус» в строке с информацией о правиле в необходимое положение (рис. 78).

Переключатель для включения/выключения правила

Рис. 78

ВНИМАНИЕ!

Чтобы изменения в правилах вступили в силу на сенсорах, использующих данную группу правил, необходимо обновить правила на данных сенсорах (п. 4.6.5.5.3 настоящего документа).

4.6.5.4.6. Удаление правил

Для удаления правила из группы правил необходимо выбрать правило, которое требуется удалить, выставив «☑» в строке с информацией о данном правиле и нажать на кнопку « 🗑 ».

ВНИМАНИЕ!

Чтобы изменения в правилах вступили в силу на сенсорах, использующих данную группу правил, необходимо обновить правила на данных сенсорах (п. 4.6.5.5.3 настоящего документа).

4.6.5.5. Управление сенсорами, использующими группу правил

4.6.5.5.1. Общая информация

Управление сенсорами, использующими группу правил, осуществляется на вкладке «Сенсоры» страницы «Администрирование» → «Группы правил» → «Группа правил» (рис. 79).

Вкладка «Сенсоры»

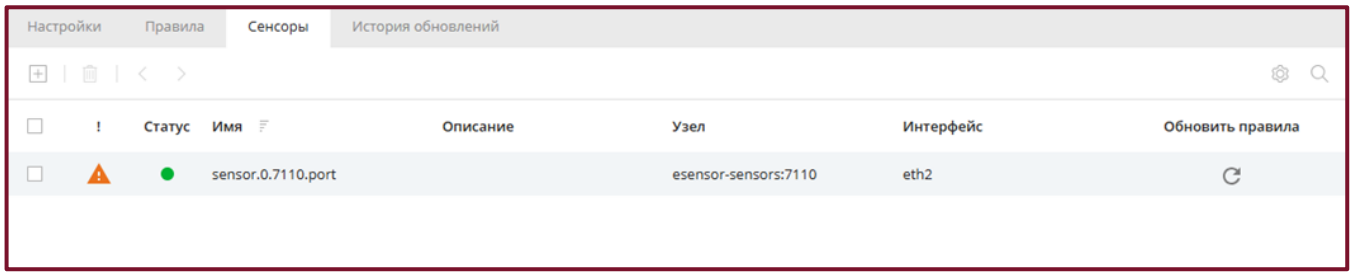

Рис. 79

Данная вкладка предоставляет возможность:

– просматривать таблицу сенсоров, использующих группу правил;
– настраивать таблицу сенсоров, использующих группу правил;
– добавлять сенсоры в таблицу сенсоров, использующих группу правил;
– обновлять правила на сенсорах;
– удалять сенсоры из таблицы сенсоров, использующих группу правил.

На данной вкладке находится информационная таблица «Сенсоры», которая содержит ту же самую информацию, что и одноименная таблица на вкладке «Сенсоры» в разделе «Дашборды (п. 4.3.4 настоящего документа), а также дополнительный столбец «Обновить правила»: если на сенсоре используется не последняя версия группы правил, в данном столбце в строке с информацией о сенсоре будет отображаться иконка «↻» (кнопка «Обновить правила сенсора»), позволяющая обновить правила на сенсоре (п. 4.6.5.5.3 настоящего документа).

4.6.5.5.2. Загрузка правил на сенсор

Для загрузки группы правил на сенсор необходимо добавить сенсор в таблицу сенсоров группы правил. Для этого необходимо нажать на кнопку « ⊞ ».

В появившемся окне (рис. 80) выбрать сенсор, который требуется добавить, выставив « ☑ » в строке с информацией о данном сенсоре. Далее нажать «Добавить».

Окно выбора сенсора

Рис. 80

ВНИМАНИЕ!

На один сенсор одновременно можно загрузить **только одну** группу правил. Чтобы загрузить на сенсор другую группу правил, необходимо сначала удалить его из списка сенсоров текущей группы.

После добавления сенсора в таблицу автоматически начнется процесс загрузки на него правил группы.

Наличие индикатора загрузки (анимированной иконки « ◌ » в столбце «Обновить правила» в строке с информацией о подключенном сенсоре в таблице на вкладке «Сенсоры» означает, что в данный момент идет процесс загрузки на него правил группы. По завершении обновления на экране появится уведомление «Обновление успешно».

4.6.5.5.3. Обновление правил на сенсоре

После обновления правил в группе правил (автоматического или по запросу пользователя), а также при изменении правил через веб-интерфейс СУС, обновленную группу правил необходимо повторно загрузить на сенсоры, использующие данную группу.

Для обновления правил на сенсоре необходимо нажать иконку « » в столбце «Обновить правила» строки с информацией о сенсоре.

Наличие индикатора загрузки (анимированной иконки « » в столбце «Обновить правила» в строке с информацией о подключенном сенсоре в таблице на вкладке «Сенсоры» означает, что в данный момент идет процесс загрузки на него правил группы. По завершении обновления на экране появится уведомление «Обновление успешно».

4.6.5.5.4. Удаление сенсора из таблицы сенсоров, использующих группу правил

При удалении сенсора из таблицы сенсоров, использующих группу правил, сенсор больше не будет использовать правила данной группы (все загруженные на него правила будут с него удалены).

Для удаления сенсора из таблицы сенсоров, использующих группу правил необходимо выбрать сенсор, который требуется удалить из списка, выставив « » в строке с информацией о данном сенсоре; нажать на кнопку « ».

4.6.5.6. Управление обновлениями группы правил

4.6.5.6.1. Общая информация

В eSensor предусмотрено два способа обновления групп правил – автоматический и по запросу пользователя.

Автоматические обновления могут происходить по заданному расписанию или в момент обновления родительской группы правил, в зависимости от выбранных настроек (п. 4.6.5.3 настоящего документа).

Создание запросов на обновление и просмотр истории обновлений осуществляется на вкладке «История обновлений» страницы «Администрирование» → «Группы правил» → «Группа правил» веб-интерфейса eSensor (рис. 81).

Вкладка «История обновлений»

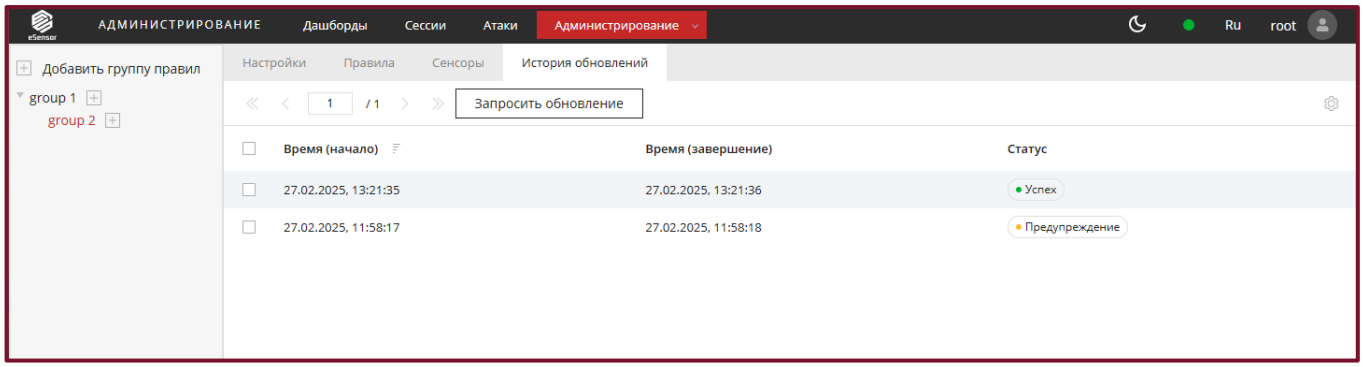

Рис. 81

Данная вкладка позволяет:

– просматривать таблицу обновлений группы правил;

– настраивать таблицу обновлений группы правил;

– создавать запросы на обновление группы правил;

– переходить к карточкам обновлений, содержащих подробную информацию об обновлениях.

В рабочей области вкладки находится таблица обновлений группы правил. По умолчанию в информационной таблице отображается информация о каждом обновлении в соответствии с таблицей 15.

Таблица 15 – Информация об обновлениях группы правил

Столбец	**Описание**
Время (начало)	Дата и время начала обновления

Столбец	Описание
Время (завершение)	Дата и время завершения обновления
Статус	Статус обновления

Обновления группы правил могут иметь один из следующих статусов:

– «Не определен» – статус обновления неизвестен;

– «Успех» – обновление успешно завершено;

– «Предупреждение» – обновление завершено с отклонениями;

– «Ошибка» – в процессе обновления произошла ошибка;

– «Загрузка» – идет загрузка правил из источника;

– «Проверка» – идет проверка правил;

– «Завершение» – идет обновление базы данных.

При обновлении группы правил загружаемые правила проходят проверку на корректность.

ВНИМАНИЕ!

Если хотя бы в одном правиле будет обнаружена ошибка, ни одно новое правило не будет загружено, а у обновления будет статус «Ошибка».

4.6.5.6.2. Создание запроса на обновление

Для создания запроса на обновление группы правил необходимо нажать кнопку «Запросить обновление». По окончании обновления на экране появится уведомление.

4.6.5.6.3. Просмотр карточки обновления

Подробная информация о каждом обновлении отображается в его карточке (рис. 82).

Карточка истории обновления

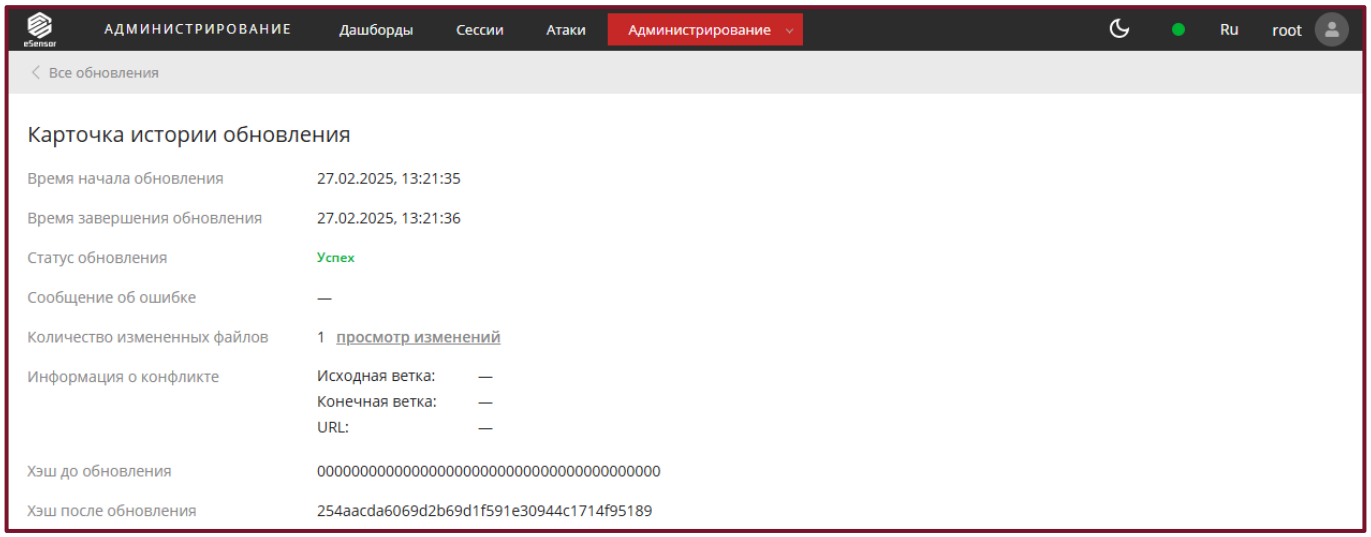

Рис. 82

Карточка содержит следующую информацию:

– время начала обновления;

– время завершения обновления;

– статус обновления;

– сообщение об ошибке, если она произошла;

– количество измененных файлов с описанием правил;

– информацию о произошедших конфликтах: названия исходной и конечной веток, содержащих файлы с правилами, а также URL внутреннего репозитория;

– хэши до и после обновления.

Для перехода к карточке обновления необходимо кликнуть по строке с информацией об обновлении таблицы обновлений группы правил.

Если кликнуть по ссылке «просмотр изменений», откроется страница с подробной информацией об изменениях, совершенных в файлах с правилами во время обновления (рис. 83).

Просмотр изменений обновления

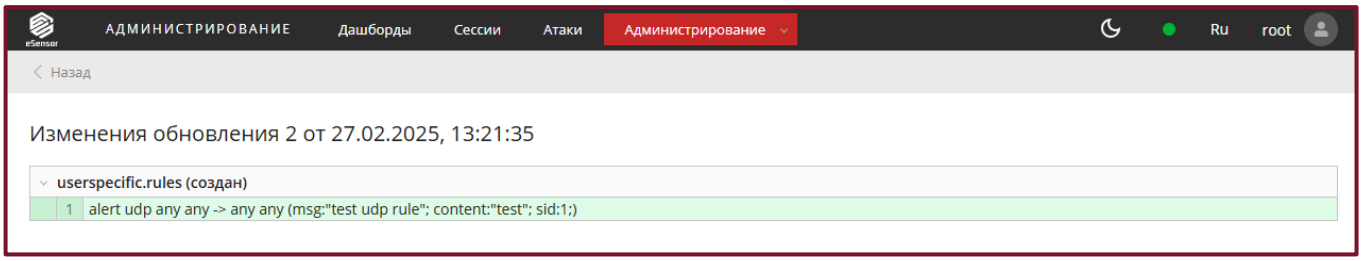

Рис. 83

Лист регистрации изменений

Изм	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводитель-ного документа и дата	Подпись	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных					