Интегрированная система обнаружения вторжений LynxLock

Руководство пользователя

LynxLock

2025 г.

научно-внедренческая компания
КОСМОСОФТ

ООО «НВК «Космософт»

Адрес: 141090, Московская область, г. Королёв, мкр. Юбилейный, ул. Маяковского, д. 2
Телефон: 8 498 500 1260
E-mail: info@kosmosoft.ru
Web: www.kosmosoft.ru

ОГЛАВЛЕНИЕ

1 ТЕРМИНОЛОГИЧЕСКИЙ СЛОВАРЬ

Сокращение	Расшифровка
ICMP	Internet Control Message Protocol – протокол межсетевых управляющих сообщений, использующийся в интернете в основном для передачи сообщений об ошибках
IP-адрес	Уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP (Internet Protocol)
SIEM	Security Information and Event Management. Решения класса SEIM предназначены для сбора событий информационной безопасности из различных источников данных
Suricata	Высокопроизводительное программное обеспечение с открытым исходным кодом для анализа сети и обнаружения угроз.
syslog	Стандарт отправки и регистрации сообщений в компьютерных сетях, работающих по протоколу IP, о происходящих в системе событиях
TCP	Transmission Control Protocol – протокол управления передачей данных в интернете, оснащен функционалом предотвращения потери данных
UDP	User Datagram Protocol – интернет-протокол пользовательских датаграмм, не обременен функционалом проверки целостности пакетов, поэтому быстрее TCP
БД	База данных
БРП	База решающих правил
демон	Программа без оконного интерфейса, находящаяся в памяти компьютера и работающая в фоновом режиме
ИСОВ	Интегрированная система обнаружения вторжений LynxLock
секрет	Информация, которую необходимо хранить в тайне для соблюдения мер информационной безопасности, например, пара «пароль – хеш пароля»
ФБО	Функции безопасности объекта

2 ВВЕДЕНИЕ

Настоящий документ содержит общее описание и инструкции по правилам работы с Интегрированной системой обнаружения вторжений LynxLock (ИСОВ).

Серверная часть системы работает под управлением ОС «Astra Linux». В ней происходит агрегирование событий безопасности и хранение их в базе данных, откуда информация забирается по запросам на узлы ИСОВ. Ядром для осуществления анализа трафика, является программное обеспечение Suricata. В качестве стартового набора правил допускается использование набора правил Emerging Threats.

Клиентская часть для взаимодействия пользователей с системой функционирует в интернет-браузере, запущенного на компьютере пользователя.

Пользователь имеет возможность одномоментно авторизоваться в системе под одной из следующих ролей:

- Администратор
- Инженер
- Оператор

В рамках своих ролей пользователям предоставляются разные права на функции системы. Администратору доступны все функции ИСОВ, Инженеру – функции управления подсистемой обнаружения вторжений + просмотр записей журналов регистрации + управление собственными данными ФБО и секретами, Оператору – только просмотр состояния и информации о зарегистрированных событиях + управление собственными данными ФБО и секретами.

3 ОБЩИЕ СВЕДЕНИЯ

3.1 Назначение

ИСОВ предназначена для обнаружения некоторых типов вредоносной активности, которые могут нарушить безопасность компьютерной системы организации, в том числе сетевых атак против уязвимых сервисов, атак, направленных на повышение привилегий, неавторизованного доступа к важным файлам, а также действий вредоносного программного обеспечения. ИСОВ использует так называемый сигнатурный анализ – поиск определенных формализованных признаков (сигнатур) в сетевых пакетах анализируемого трафика. Сигнатуры – формализованные признаки и описания связанных с такими признаками вредоносной сетевой активности хранятся в БРП.

ИСОВ является клиент-серверной системой с интерфейсом пользователя, выполненном в виде веб-приложения, и серверной частью.

3.2 Функционал системы

В ИСОВ реализованы:

- Идентификация и аутентификация пользователя;
- Разделение прав доступа пользователей с использованием ролевой модели;
- Возможность управления (запуск, остановка, просмотр состояния) из веб-интерфейса;
- Контроль целостности исполняемых файлов и наборов правил;
- Автоматическое обновление базы решающих правил;
- Встроенный редактор для собственных правил;
- Возможность управления и настройки для иерархически подчиненных узлов из одной точки;
- Передача данных о событиях безопасности с подчиненных узлов на контроллер;
- Передача данных о событиях безопасности по syslog на внешние SIEM-системы;
- Регистрация внутренних (связанных с функционированием ИСОВ) событий безопасности;
- Анализ зарегистрированных событий безопасности по интегральным и дифференциальным характеристикам, в том числе с привязкой к геолокации адреса источника;
- Формирование отчетов о событиях безопасности за заданный период.

3.3 Входные и выходные данные

В качестве входных данных ИСОВ выступают сетевой трафик и решающие правила. БРП хранится на сервере с установленной ИСОВ, а обновления БРП доступны на сервере обновлений ИСОВ. Также входными данными ИСОВ являются конфигурационные параметры ИСОВ.

В качестве выходных данных системы ИСОВ выступают:

- Данные о факте обнаружения атаки с идентификацией события (потенциальной атаки/вторжения) с оповещением пользователя (администратора);
- Дублирование данных о событии (потенциальной атаке/вторжении) по электронной почте;
- Данные по зарегистрированным событиям (атакам/угрозам) для детального анализа (журнал регистрации угроз);
- Данные о контроле состояния ядра анализатора трафика (производительность, статистика по зарегистрированным угрозам, в т.ч. в графическом виде, инструменты фильтрации и поиска);
- Данные о результатах мониторинга состояния интерфейсов захвата трафика.

3.4 Подсистемы ИСОВ

В качестве дополнительных блоков в СОВС и СОВУ присутствуют подсистемы:

- Подсистема Ядра анализатора;
- Подсистема Агента (обеспечивает сбор данных);
- Подсистема БД;
- Подсистема Регистрации событий;
- Подсистема WebGUI (формирует интерфейс для конечного пользователя).

Взаимодействие экземпляров ИСОВ показано на рисунке ниже.

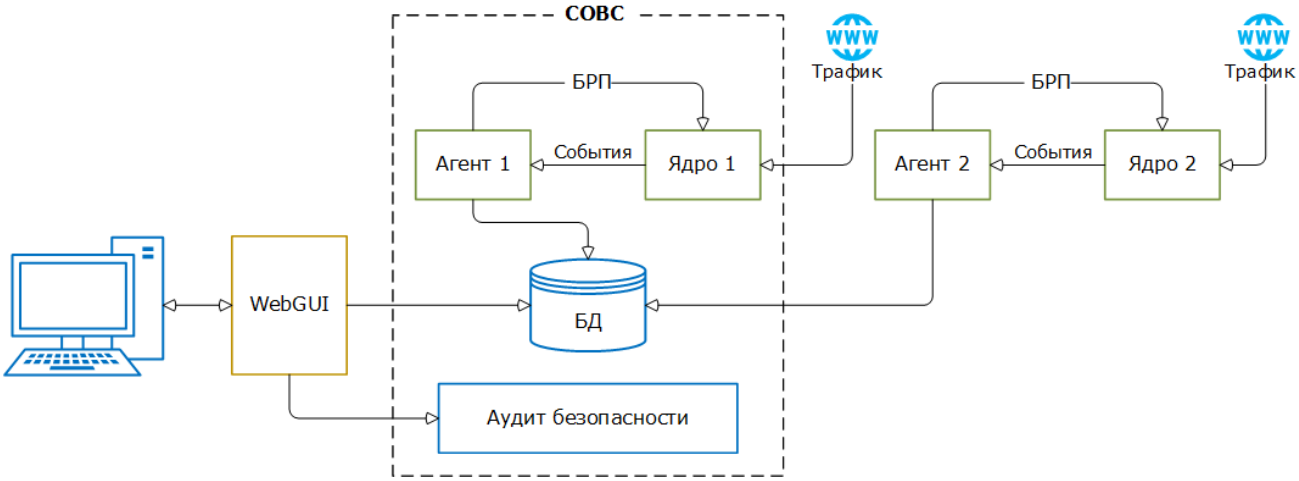

Рисунок 3.1 Схема взаимодействия подсистем ИСОВ

3.5 Основы интерфейса

Интерфейс системы выполнен в современном стилевом решении, интуитивно понятном для большинства пользователей.

3.5.1 Навигация

В левом меню находится содержание, иерархическая структура разделов, доступных той роли пользователя, под которой он авторизовался. Если раздел первого уровня содержит подразделы, то справа от его названия присутствует значок  . Клик по названию раздела открывает список его подразделов. Пример открытого родительского раздела «Отчеты»:

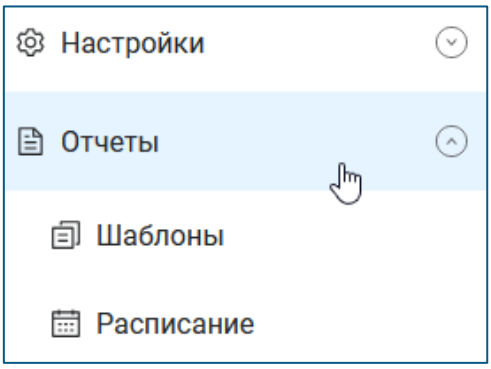

Рисунок 3.2 Родительский раздел «Отчеты» в левом меню

Левое меню можно сворачивать в компактный вид по кнопке  :

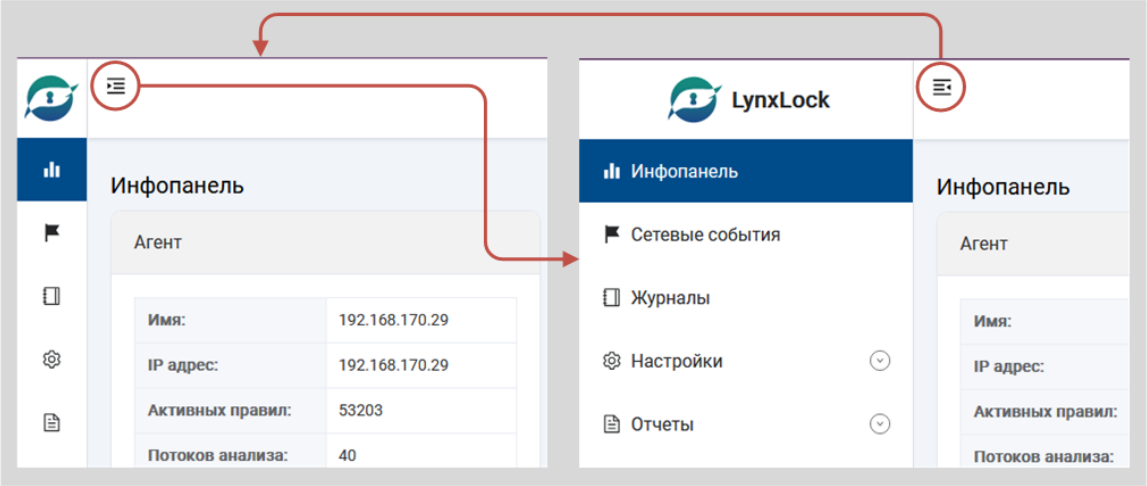

Рисунок 3.3 Сворачивание/разворачивание левого меню

3.5.2 Таблицы

Если страница подразумевает размещения на ней списка однотипных сущностей, то, как правило, используется таблица. Например, сетевые события:

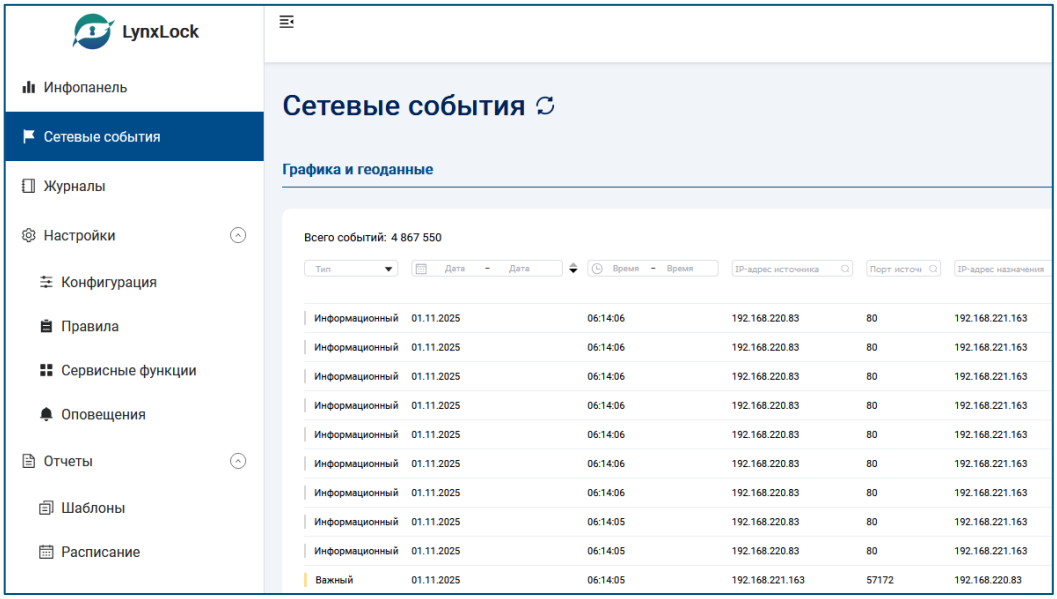

Рисунок 3.4 Таблица в системе

На что здесь обратить внимание:

- **Фильтрация**. Над таблицей располагаются поля фильтров, благодаря которым набор данных в таблице можно сократить до необходимого минимума. В таблице останутся только записи, удовлетворяющие фильтру.
- **Ранжирование**. Можно менять порядок отображения записей списка по тому или иному столбцу. Если столбец в своем названии содержит пиктограмму , то по нему можно ранжировать. В этой пиктограмме обе стрелочки кликабельны и отвечают за направление сортировки.
- **Скроллинг**. Перемещение по таблице в вертикальном направлении осуществляется путем прокрутки колесика мыши или клавиатурными стрелками «Вверх» или «Вниз». Подтягивание новых строк в таблицу происходит по мере прокрутки.

3.5.3 Формы

Многие формы, служащие для добавления и редактирования сущностей системы, обладают одинаковыми элементами управления, среди которых:

- Строковая кнопка «Добавить» или графическая кнопка «+». Для добавление определенного параметра сущности, например, Правила или Получателя, который выбирается или назначается моментом ранее.
- Графическая кнопка  . Для открытия окна редактирования параметра сущности.
- Графическая кнопка  или  . Для удаления параметра сущности.
- Кнопка «Сбросить». Для очистки полей формы, измененные в текущей сессии формы.
- Кнопка «Отмена». Для закрытия формы без сохранения изменений.

4 ПОДГОТОВКА К РАБОТЕ

4.1 Общая последовательность действий

Для подключения и идентификации/аутентификации в веб-интерфейсе ИСОВ необходимо выполнить следующую последовательность действий:

- дождаться загрузки операционной системы на АРМ пользователя;
- запустить интернет-обозреватель;
- ввести в адресной строке интернет-обозревателя URL системы, полученный от системного администратора;
- совершить клик по центральной пиктограмме;
- в открывшейся форме авторизации ввести логин и пароль.

Если программа загрузилась без ошибок, то в окне интернет-обозревателя откроется интерфейс ИСОВ, соответствующий роли пользователя.

4.2 Выход из программы

Для выхода из системы недостаточно закрыть окно браузера или вкладку браузера – в этом случае согласно настройкам браузера по умолчанию авторизация и сеанс работы с ИСОВ будут сохранены и в следующем заходе в ИСОВ авторизации не потребуется.

Если же воспользоваться штатным выходом, то сеанс будет закрыт и в следующий заход потребуется новая авторизация, что является более безопасным сценарием работы с системой. Штатный выход осуществляется через пункт «Выход» в меню, которое открывается по клику на блок пользователя в верхнем правом углу интерфейса:

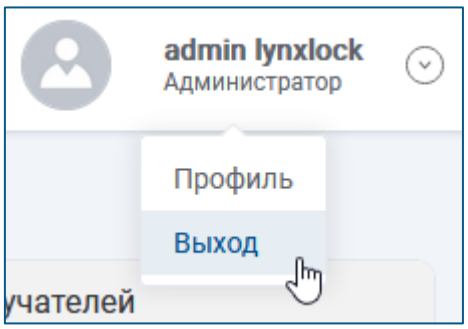

Рисунок 4.1 Выход из системы

5 ВЫПОЛНЕНИЕ ПРОГРАММЫ

5.1 Инфопанель

После успешной авторизации пользователь попадает на стартовую страницу системы, которой является «Инфопанель». Страница содержит виджеты:

- Агент. В виджете отображаются данные о демоне, который занимается мониторингом логов системы по решающим правилам. Статус агента, количество активных правил, потребление серверных ресурсов…
- Счетчик событий. За определенный период отображается статистика событий. Период назначается на странице, открываемой по пути: Настройки > Конфигурация > События.
- Топ IP-адресов источников. Графическое и табличное представления Топ-10 самых активных источников трафика с указанием количества событий. За период.
- Топ IP-адресов получателей. Графическое и табличное представления Топ-10 самых активных получателей трафика с указанием количества событий. За период.
- Коды событий (идентификаторы сигнатур). Указаны абсолютные и относительные данные по Топ-10 кодов событий (правил).

Внешний вид виджетов представлен ниже:

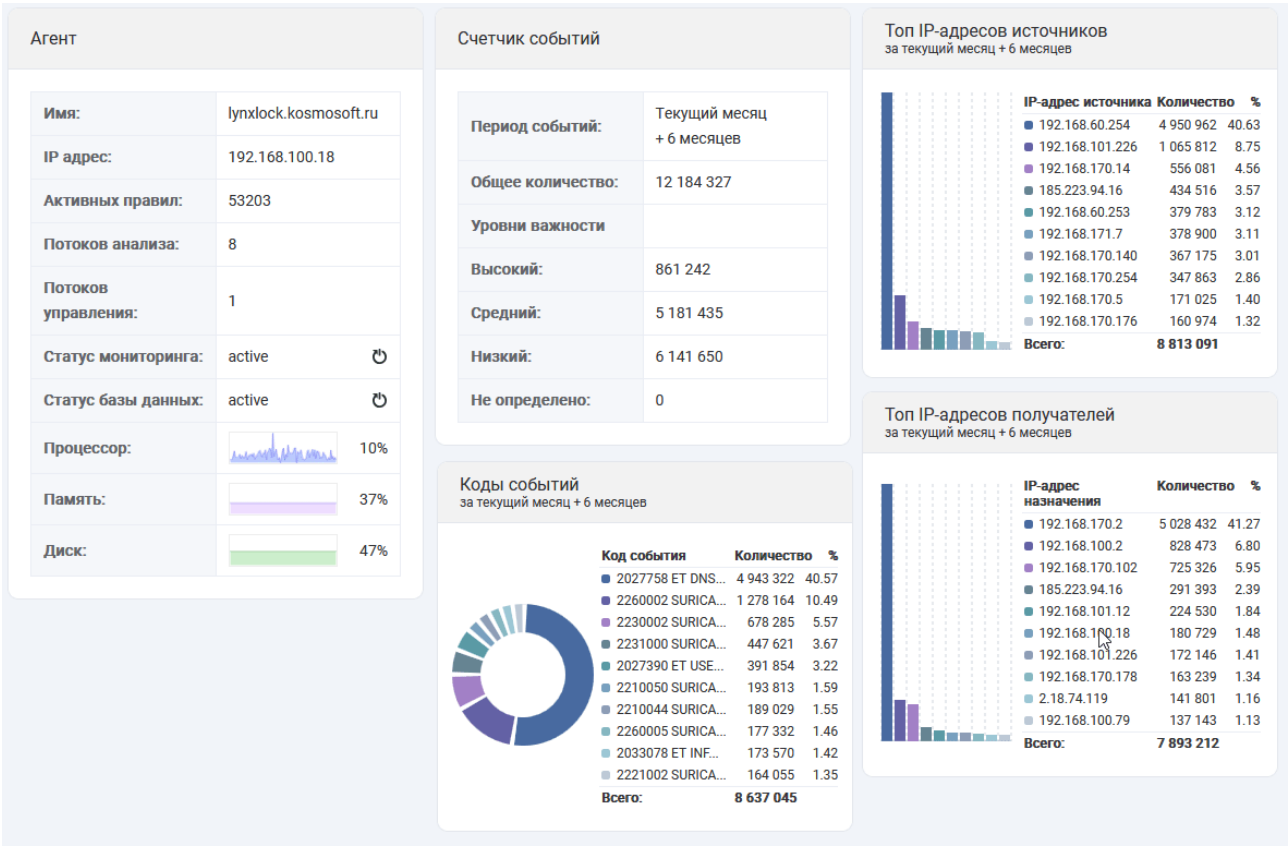

Рисунок 5.1 Виджеты инфопанели

5.2 Сетевые события

5.2.1 Табличное представление

Основной таблицей, аккумулирующей данные о результатах анализа трафика в ИСОВ, является таблица «Сетевые события».

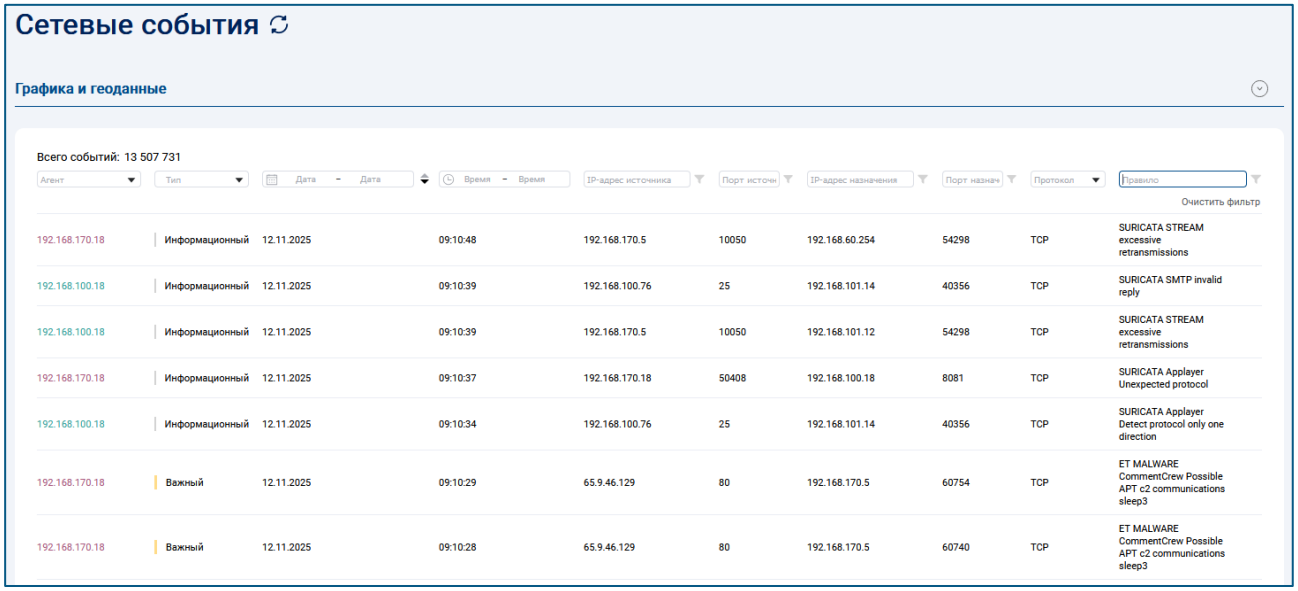

Рисунок 5.2 Сетевые события

Таблица обладает фильтрами, за счет которых выборка событий детализируется. Возможно применять следующие фильтры:

- Агент. Выбор агента по IP.
- Тип. Выбор события из «Важный», «Незначительный», «Информационный». По умолчанию показываются все типы.
- Дата. Выбор периода между двумя датами, в который зафиксировано событие.
- Время. Выбор времени между двумя значениями, в которое зафиксировано событие.
- IP-адрес источника. Указание IP или части IP источника события.
- Порт источника. Указание номера порта отправляющего устройства.
- IP-адрес назначения. Указание IP или части IP получателя события.
- Порт назначения. Указание номера порта принимающего устройства.
- Протокол. Выбор из TCP, UDP, TCMP.
- Правило. Указание текстового контекста, содержащегося в названии правила. Для применения этого фильтра надо после набора контекста нажать клавишу Enter.

Если задать какие-то значения в разных полях фильтра, то условия этих фильтров будут отрабатываться по логике «И».

При наведении курсора мыши на значение ячейки столбца (у которого в шапке есть иконка) пользователь может увидеть кнопки (+) и (–). Эти кнопки служат для добавления данного значения в фильтр столбца или исключения данного значения из выборки таблицы.

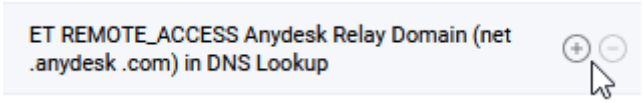

Рисунок 5.3 Добавление/исключение значения ячейки в фильтре

При этом по кнопке в фильтре столбца можно просмотреть исключенные/добавленные значения:

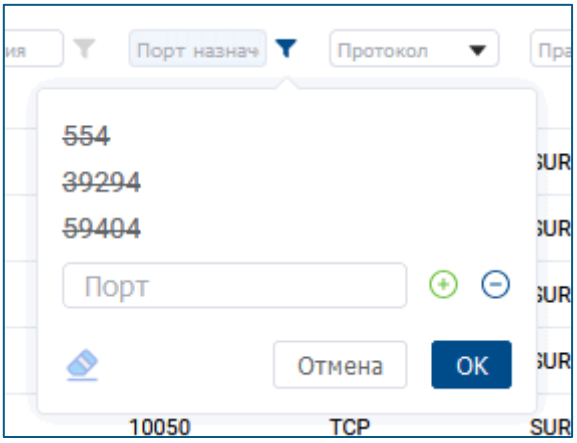

Рисунок 5.4 Фильтр с исключенными значениями

В окне, вызываемом по кнопке ▼, также есть кнопки (+) и (–). Набирая в поле ввода то или иное значение и нажимая ту или иную кнопку можно формировать фильтр, который будет действовать согласно логическому «И».

Для сброса фильтрации таблицы служит ссылка «Очистить фильтр», размещенная под строкой фильтров справа.

5.2.2 Графическое представление

На странице «Сетевые события» есть не только табличное представление данный, но и графическое. В верхней строке «Графика и геоданные» справа находится иконка ⌄, которая отвечает за переход к графикам. Перед этим переходом надо выбрать агента в первом поле фильтров. Графики отобразят содержание таблицы с учетом примененных фильтров.

Итак, в графике пользователь может увидеть Дифференциальный график, Интегральный график и Геоданные. График располагается над таблицей, поэтому возможно пролистать страницу вниз, чтобы на ходу внести изменения в нее для перерисовки графика.

Дифференциальный график. Это классический график на котором в зависимости от времени показано количество событий того или иного характера в виде скользящего среднего. Над графиком справа есть кнопки для изменения масштаба и для сохранения графика в виде растрового изображения. Под графиком есть поля нескольких фильтров.

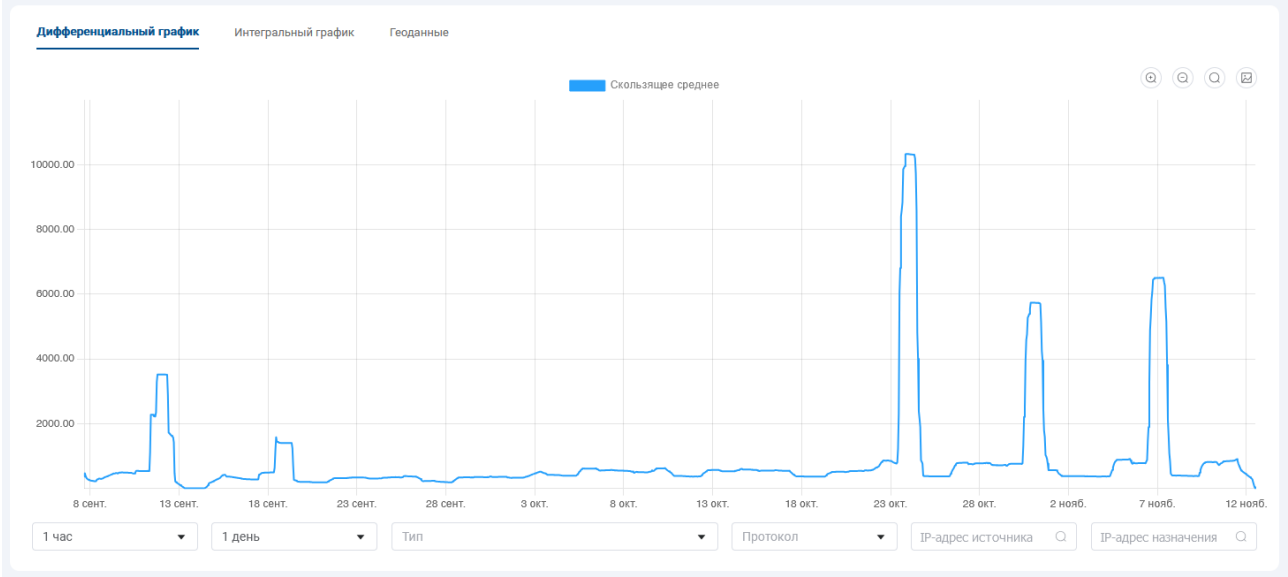

Рисунок 5.5 Дифференциальный график

При наведении мыши на участок графика возникает подсказка по точке на кривой:

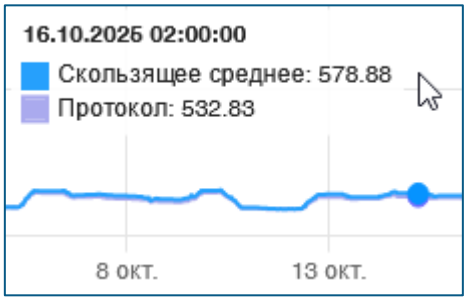

Рисунок 5.6 Информация о точке на кривой графика

Интегральный график. На таком графике показаны суммарные данные событий по Важности, Протоколам, Источникам или Получателям. Переключение между сущностями интереса находятся под графиком слева.

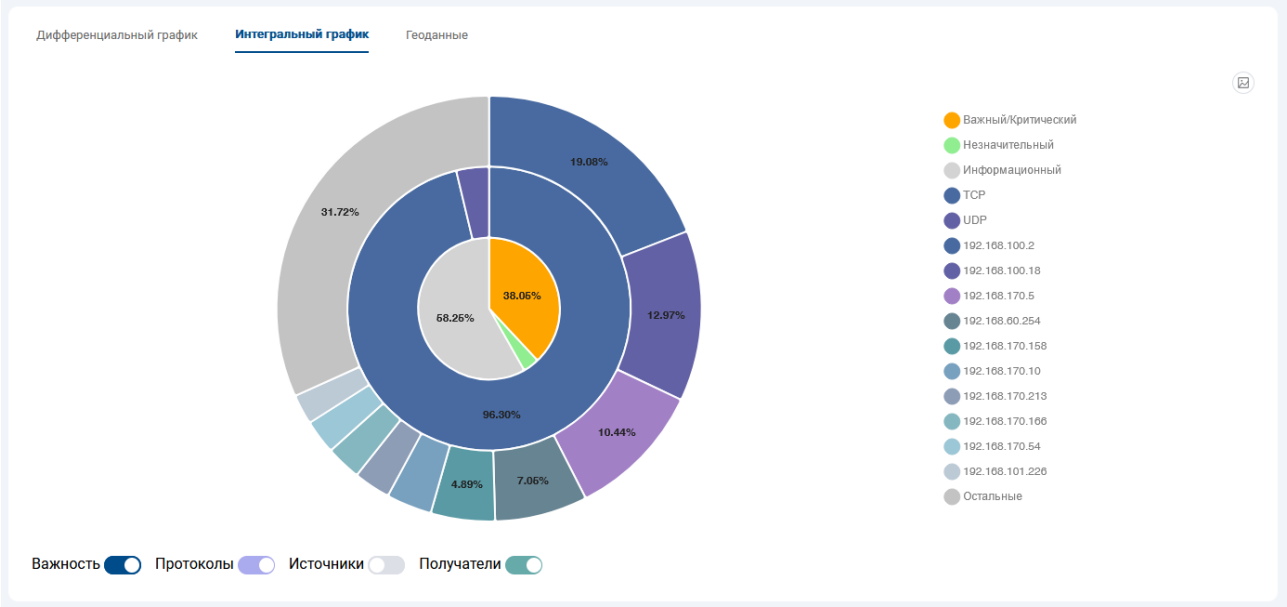

Рисунок 5.7 Интегральный график

Сущности интереса можно включать одновременно. По кнопке  график экспортируется в растровое изображение.

График геоданных. На этом графике показано распределение событий на карте мира по Источникам, Получателям или Интенсивности.

Рисунок 5.8 График "Геоданные"

Переключение между сущностями интереса осуществляется по переключателям под графиком слева.

5.3 Журналы

На странице представлены закладки «Контрольная подсистема», «Агент», «Агрегатор», «Средство мониторинга», «База данных» и «Авторизация». Журналы предназначены для регистрации событий безопасности ИСОВ с возможностью просмотра и фильтрации.

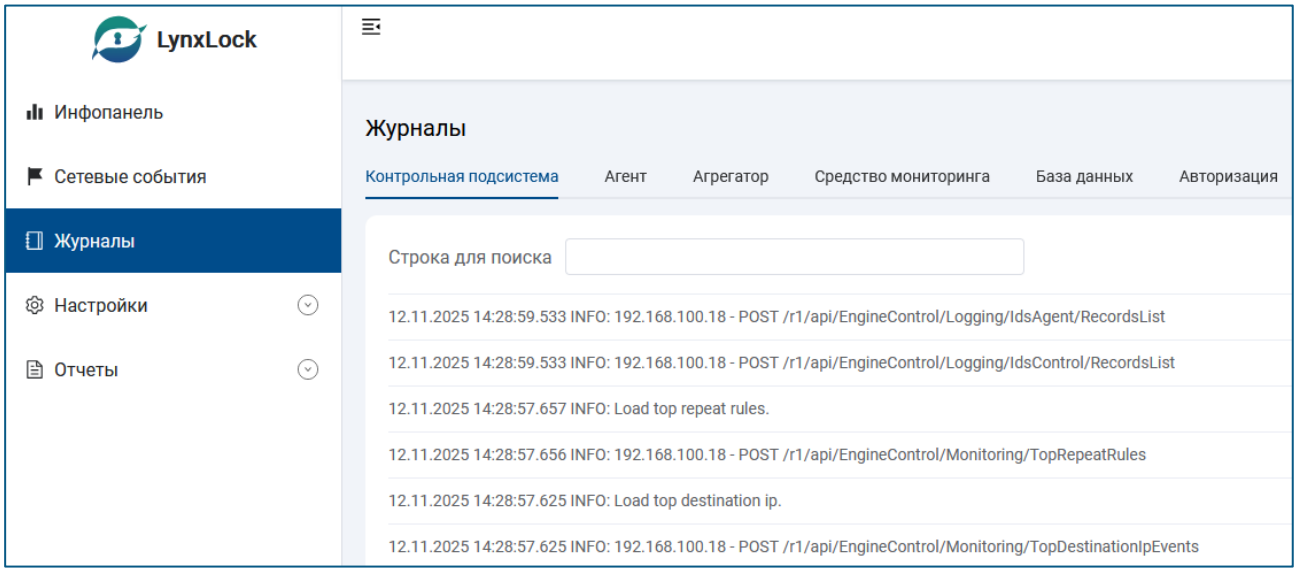

Рисунок 5.9 Журналы

> **Примечание**. Регистр в фильтре имеет значение.

5.4 Настройки

5.4.1 Конфигурация

В этом подразделе находятся вкладки для редактирования конфигурации системы: «Параметры», «Логирование», «События», «Геоданные» и «SMTP».

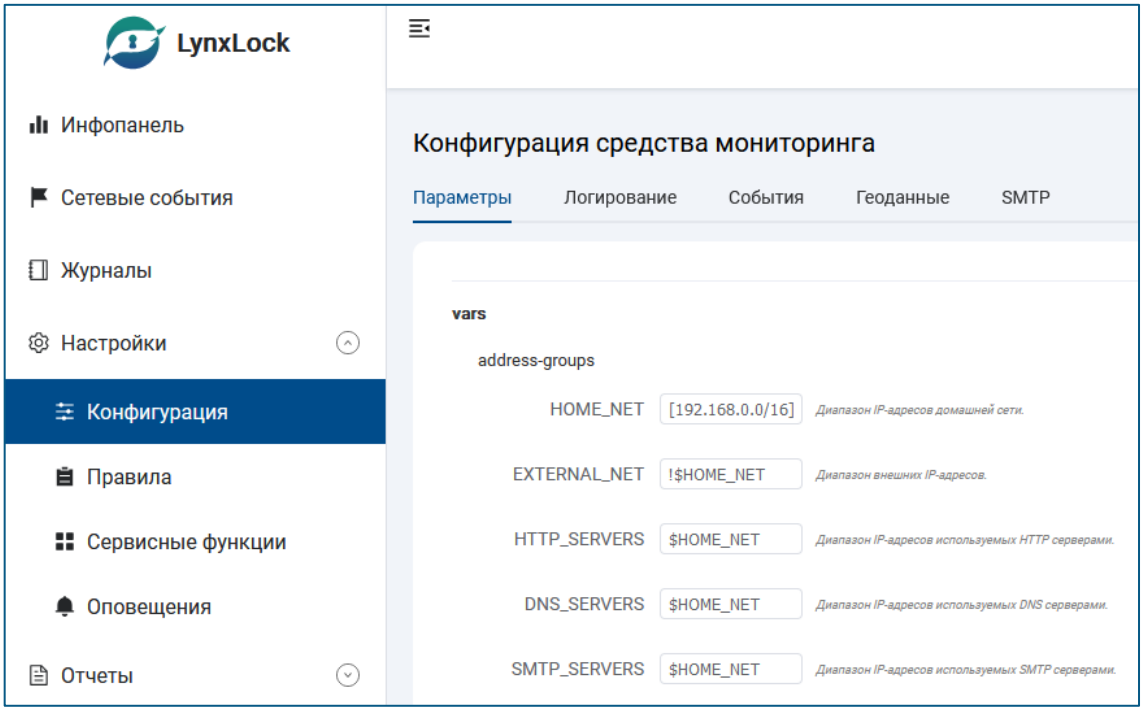

Рисунок 5.10 Настройки > Конфигурация > Параметры

На закладке «Параметры» указываются подсети для применения специальных политик анализа.

Основной переменной, определяющей такие подсети, является $HOME_NET. В переменной хранится подсеть, соответствующая домашней сети ИСОВ. Все внешние IP-адреса находятся в переменной $EXTERNAL_NET, которая определяется как !$HOME_NET.

На закладке «Логирование» включается или выключается запись логов в файл на сервер или на локальный компьютер с указанием его IP-адреса и порта сервера. Можно выбрать тип событий из «Важный», «Незначительный», и «Информационный». Невыбор типа означает все типы. Имя файла с логами назначается на закладке «Параметры» в поле «filename» группы «outputs».

На закладке «События» находится:

- Информация по занимаемому логами событий места на диске.
- Выбор периода, за какой будут отображаться данные в виджете «Счетчик событий» инфопанели.

На закладке «Геоданные» находится:

- Информация о количестве подсетей с привязкой к географии и дате последнего обновления.
- Функционал загрузки на сервер файла с геоинформацией (соответствие IP местоположению).

На закладке SMTP находятся настройки почтового сервера для рассылки сообщений.

5.4.2 Правила

В этом подразделе находятся вкладки для работы с правилами: «Кэш» и «Инициализация».

Правило/сигнатура состоит из следующих элементов:

- Действие, определяющее, что происходит при срабатывании правила.
- Заголовок, определяющий протокол, IP-адреса, порты и направление правила.
- Параметры правила, определяющие специфику правила.

События в логах отбираются согласно правилам. Пример правила:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http.method; content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-unknown; sid:123; rev:1;)
```

Здесь:

alert – действие.

$HOME_NET any -> $EXTERNAL_NET any – заголовок с указанием направления трафика.

msg:"HTTP GET Request Containing Rule in URI"; flow:established,to_server; http.method; content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-unknown; sid:123; rev:1; – параметры, по которым будут вычленяться события.

По умолчанию подраздел открывается на закладке «Кэш»:

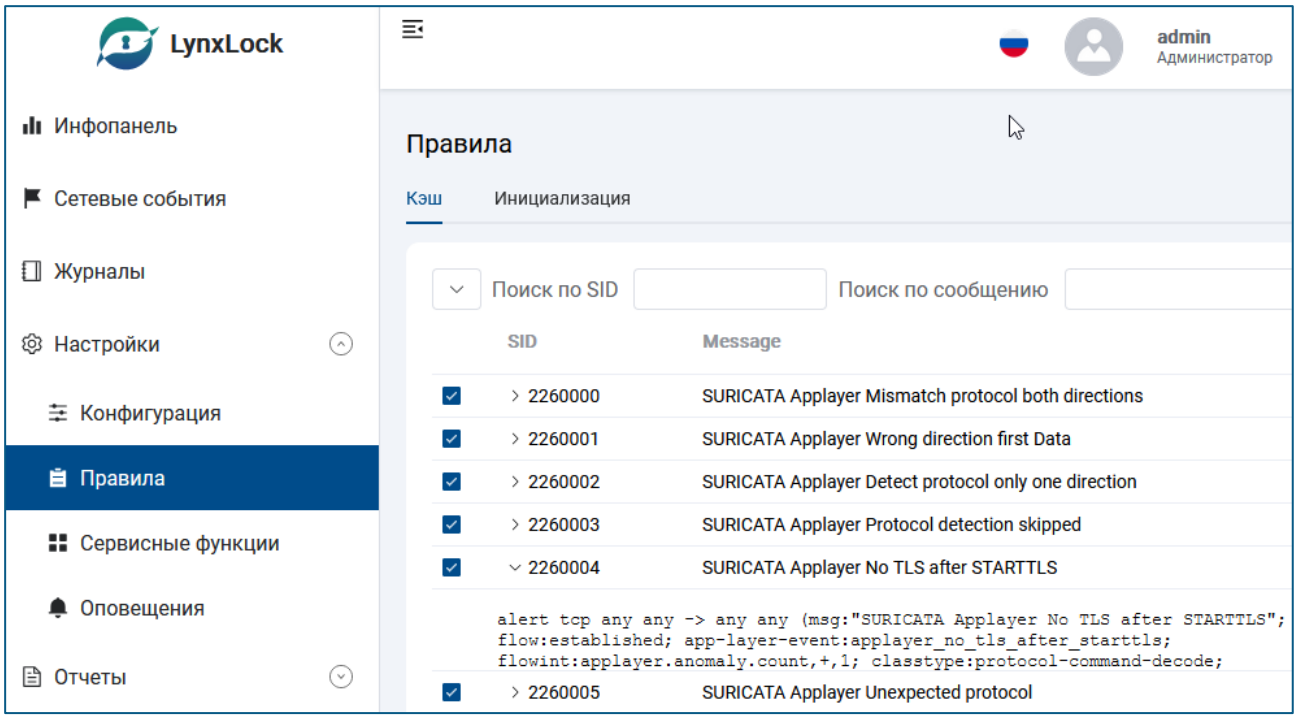

Рисунок 5.11 Настройки > Правила > Кэш

На закладке «Кэш» действующие правила Suricata можно просматривать с фильтром и без, а также включать/отключать правила. Фильтр возможен по двум параметрам правила: sid и msg. Кнопка служит для отображения или включенных правил, или отключенных.

На закладке «Инициализация» находится функционал для загрузки правил из файла на сервер.

5.4.3 Сервисные функции

В этом подразделе проводится проверка конфигурации и контрольных параметров системы с отображением результата проверки.

5.4.4 Оповещения

В этом подразделе назначаются получатели сообщений Сетевых событий и Состояний агента.

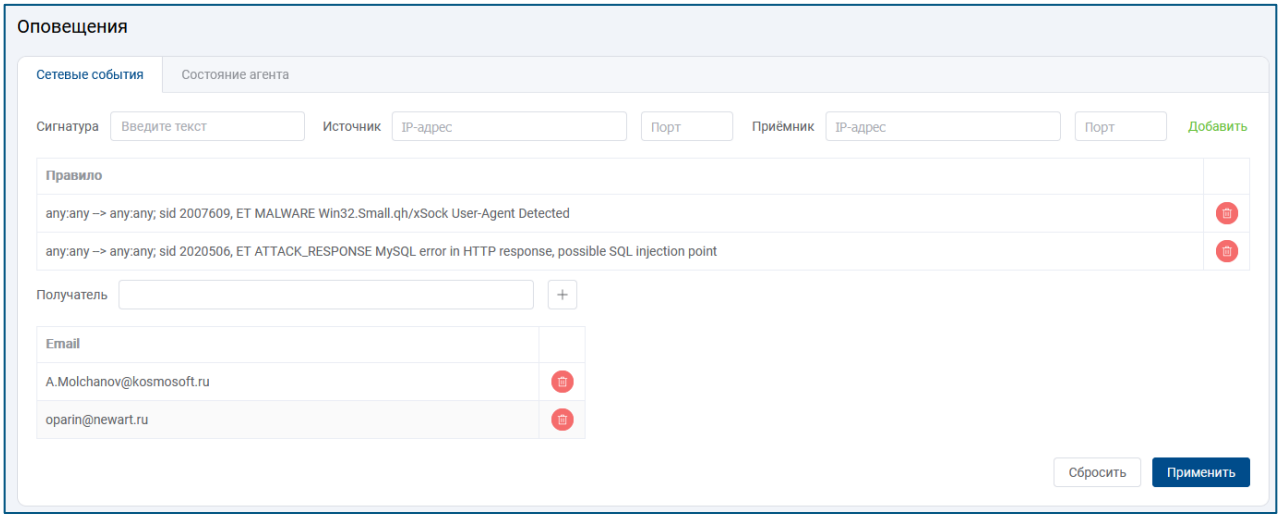

Рисунок 5.12 Настройки > Оповещения > Сетевые события

На закладке «Сетевые события» можно выбрать правило по Сигнатуре, Источнику, Приемнику и для этого (этих) правила назначить получателя сообщений.

Для выбора правила надо ввести контекст в поле «Сигнатура» и из предложенного списка выбрать нужное. При необходимости – добавить IP-адрес и Порт Источника/Приемника. После этого нажать кнопку «Добавить» справа. Правило появится в списке «Правило».

Для выбора получателя сообщений – набрать его e-mail в поле «Получатель» и нажать кнопку «+» справа от этого поля. Получатель появится в списке «Email».

Правило и Получателя из своих список можно удалить по кнопке .

Для принятия произведенных изменений следует нажать кнопку «Применить».

Кнопка «Сбросить» служит для отмены произведенных изменений в текущей сессии работы с формой.

Оповещение приходит на e-mail получателя по факту фиксирования события.

На закладке «Состояние агента» настраиваются параметры, по факту превышения которых получателю будет отправляться сообщение на его e-mail. Параметры снабжены подсказкой. После завершение редактирования полей следует нажать кнопку «Применить» для запоминания настроек.

Кнопка «Сбросить» служит для отмены произведенных изменений в текущей сессии работы с формой.

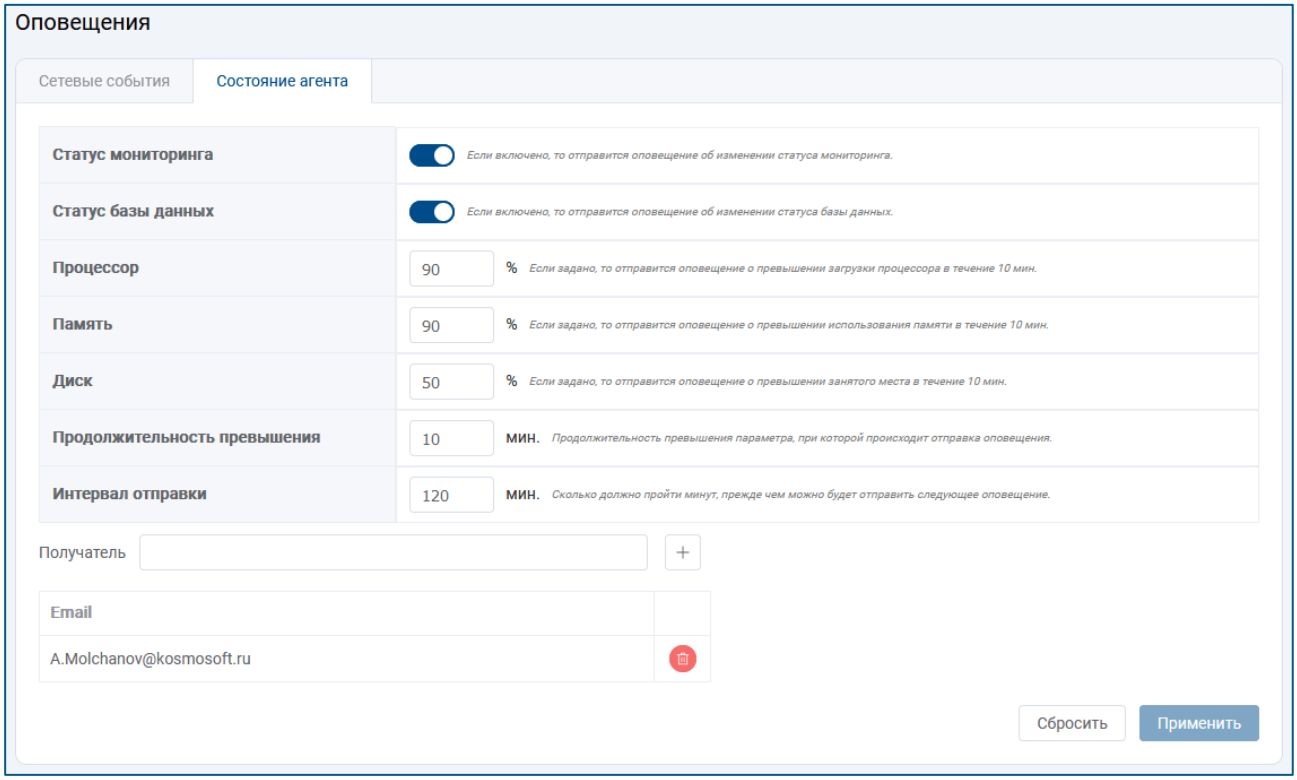

Рисунок 5.13 Настройки > Оповещения > Состояние агента

5.5 Отчеты

5.5.1 Шаблоны

В этом подразделе добавляются, редактируются и хранятся шаблоны отчетов. А также генерятся и скачиваются отчеты. При нажатии на кнопку-стрелку «>» открывается плашка с кнопкой «Сформировать отчет» и ссылкой «Количество отчетов», по клику на которую появляется список ранее сформированных отчетов:

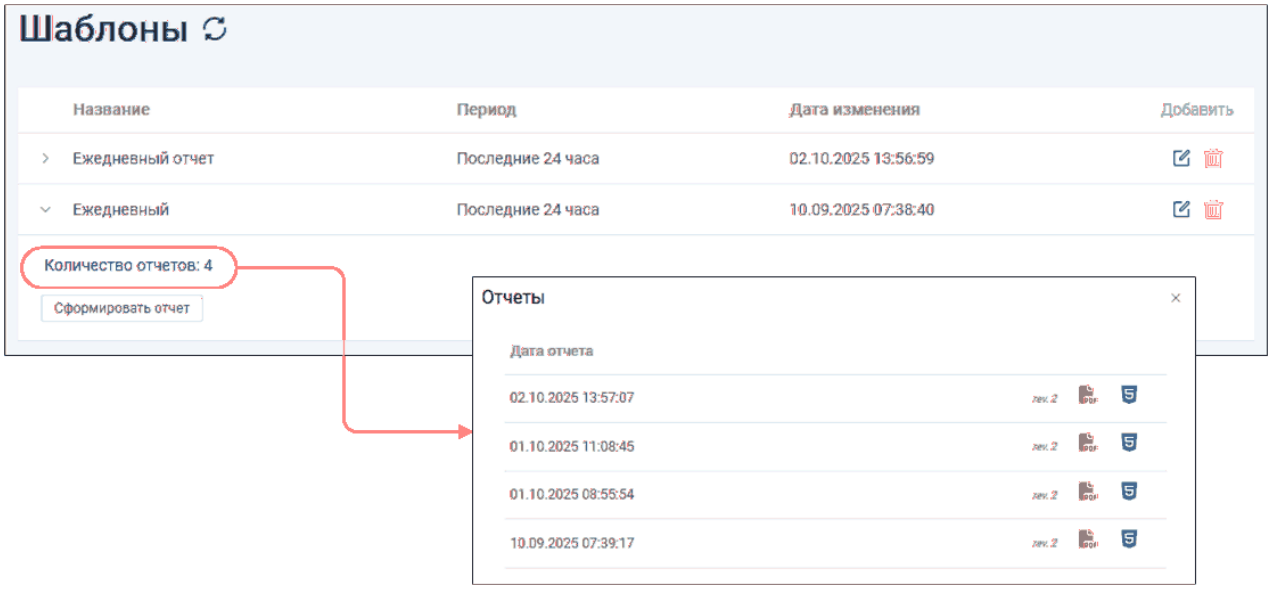

Рисунок 5.14 Отчеты > Шаблоны

Из данного списка отчет можно скачать в формате PDF (кнопка) или HTML (кнопка).

Добавляется шаблон по кнопке «Добавить».

Редактируется шаблон по кнопке .

Добавление и редактирование происходит в форме:

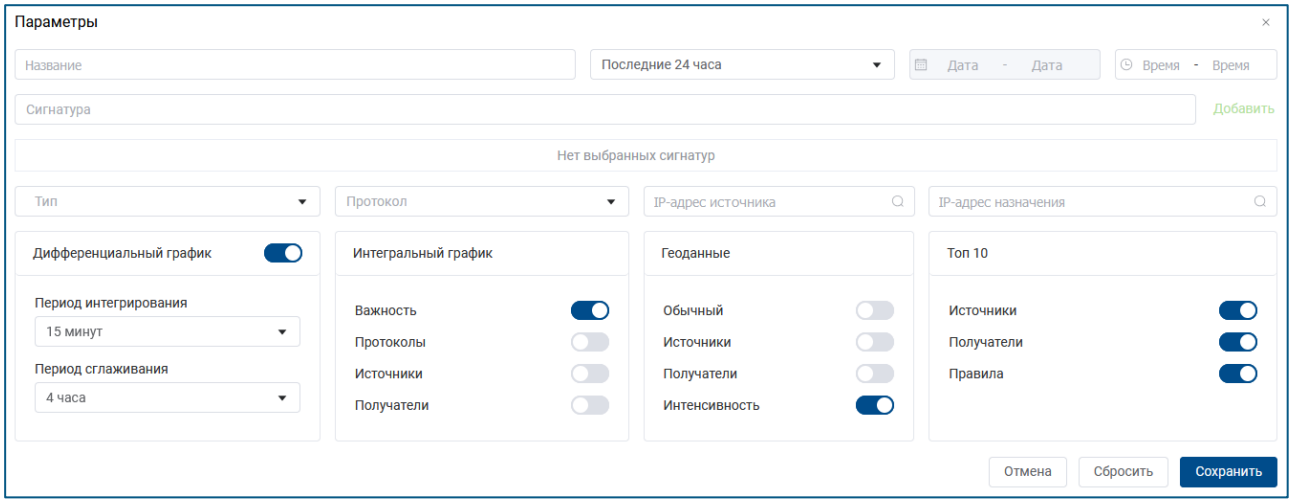

Рисунок 5.15 Форма добавления/редактирования шаблона отчета

В этой форме присутствуют поля:

- Название. Пишется текст в произвольной форме, который будет фигурировать в списке шаблонов.
- Последние 24 часа. Период снятия данных. Возможные значения: «Точная дата», «Последние 24 часа» (по умолчанию), «Последние 7 дней» и «Последние 30 дней».
- Дата. Поле активно для выбора даты или диапазона дат при выборе периода «Точная дата».
- Время. Выбор периода времени суток.
- Сигнатура. Контекст для поиска правила. При выборе правила следует нажать на кнопку «Добавить» и правило появится в списке правил на месте поля «Нет выбранных сигнатур».
- Тип. Выбор события из «Важный», «Незначительный», «Информационный». По умолчанию учитываются все типы.
- Протокол. Выбор из значений: TCP, UDP и ICMP.
- IP-адрес источника. IP источника события.
- IP-адрес назначения. IP получателя события.
- Дифференциальный график. Показ количества событий в единицу времени с учетом периода интегрирования и периода сглаживания. Период интегрирования – это точка на графике, соответствующая количеству событий за этот период.
- Интегральный график. Суммарные данные событий по одному или нескольким параметрам: «Важность», «Протоколы», «Источники» и «Получатели».
- Геоданные. Карта мира с прорисовкой геолокации событий по параметрам: «Обычный», «Источники», «Получатели» и «Интенсивность».
- Топ 10. Секторная диаграмма-бублик, на которой отображаются коды событий (названия правил) с учетом: «Источники», «Получатели» и/или «Правила».

Удаляется шаблон по кнопке .

5.5.2 Расписание

В этом подразделе составляется и редактируется расписание рассылок отчетов по адресатам.

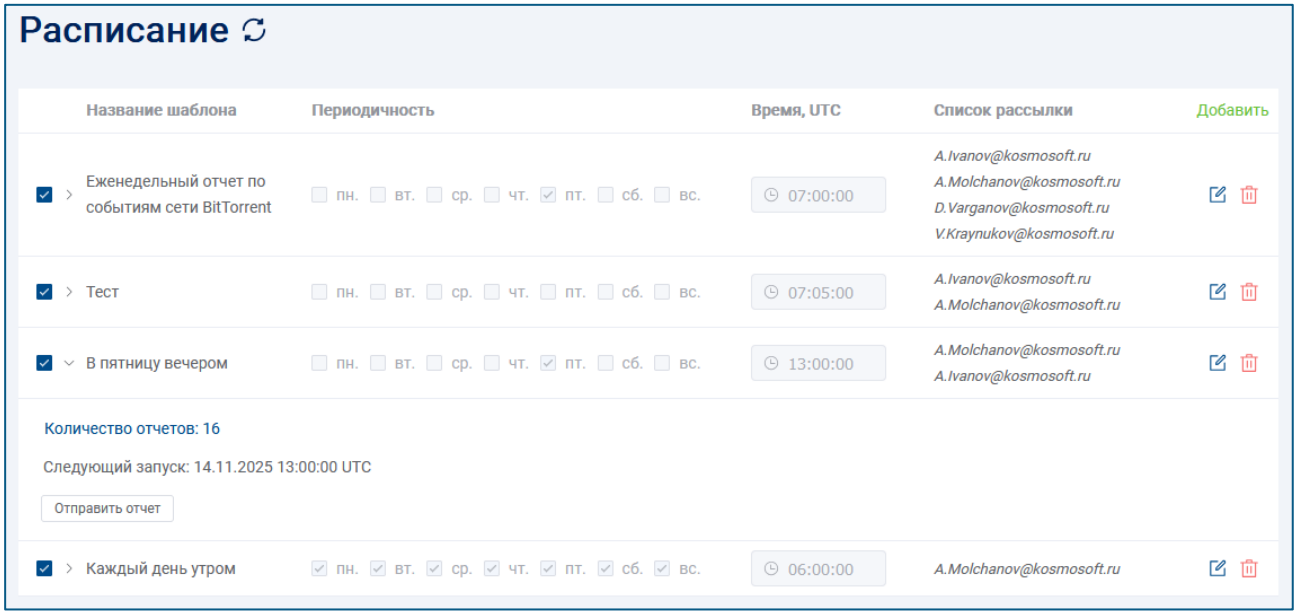

Рисунок 5.16 Отчеты > Расписание

Чтобы составить новое расписание следует нажать на кнопку «Добавить». Откроется окно:

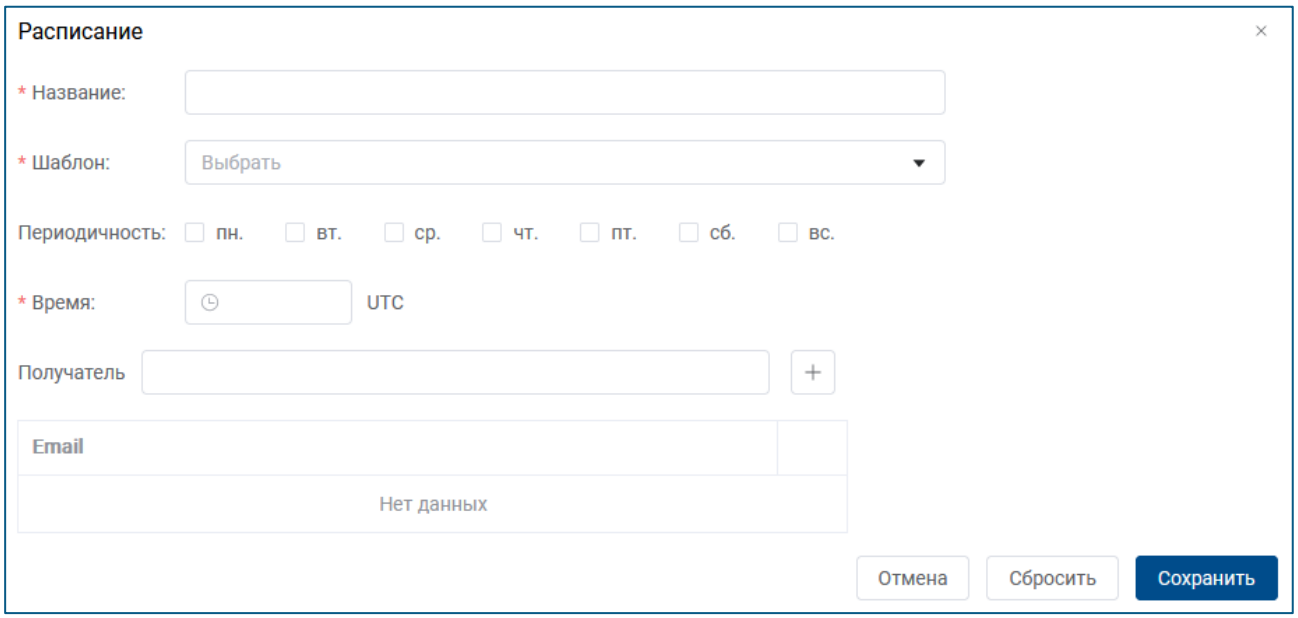

Рисунок 5.17 Форма добавления расписания

В форме надо дать название расписанию, выбрать именованный шаблон отчета, указать периодичность рассылки по дням недели, задать время рассылки, назначить получателей в виде их email-адресов и нажать кнопку «Сохранить».

Кнопка «Сбросить» служит для очитки полей формы.

Кнопка «Отмена» служит для закрытия формы без сохранения данных.

Редактируется расписание по кнопке .

Удаляется расписание по кнопке .