
# Руководство администратора

Версия документа от 18 мая 2020 года

# Аннотация

Настоящее Руководство администратора описывает набор мероприятий и действий для настройки и эксплуатации Системы контентной фильтрации веб трафика (далее - СКФВТ) Наименование заказчика.

# Содержание

# Перечень условных обозначений, терминов и сокращений

| Обозначение | Описание |
|---|---|
| CIDR | Classless Inter-Domain Routing – формат описания IP-адресации |
| DLP | Data Leak Prevention — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне |
| DOCX | Формат файлов, представляющий собой модернизированную версию формата DOC. Используется программами Microsoft Word 2007, 2010, 2013 и 2016 для Windows, а также Microsoft Word 2008 и 2011 для Mac OS X |
| ICAP | Internet Content Adaptation Protocol – протокол интеграции с DLP системой |
| IP | Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP |
| FQDN | Fully Qualified Domain Name – уникальное доменное имя ресурса |
| LDAP | Lightweight Directory Access Protocol – облегченный протокол для доступа к службе каталога |
| MIB | Management Information Base – перечень доступной информации для мониторинга |
| NTP | Network Time Protocol — протокол сетевого времени |
| PDF | Универсальный файловый формат, который позволяет сохранить шрифты, изображения и сам макет исходного документа независимо от того, на какой платформе и в каком приложении такой документ создавался |
| SNMP | Simple Network Management Protocol. Протокол, который используется для получения статистических параметров работы устройства |
| SPN | Service Principal Name. Первичное имя сервиса, которое используются для идентификации сервера с установленными на нём сервисами |
| SSL | Secure Sockets Layer – криптографический протокол, который обеспечивает защищенную передачу информации в Интернете |
| SSH | Secure Shell – протокол защищенного подключения |
| TCP | Transmission Control Protocol – протокол управления передачей данных |
| АРМ | Автоматизированное рабочее место |
| Заказчик | Наименование заказчика |
| ОС | Операционная система |

| Обозначение | Описание |
|---|---|
| ПО | Программное обеспечение |
| Исполнитель | Наименование исполнителя |
| СКФВТ<br>Система | Система контентной фильтрации веб трафика |

# 1 Введение

## 1.1 Общие сведения

**Полное наименование системы:** Система контентной фильтрации веб трафика.
**Условное обозначение системы:** СКФВТ.

Перед эксплуатацией СКФВТ обслуживающему персоналу необходимо ознакомиться со следующими документами:

- «Пояснительная записка»;
- «Руководство администратора»;
- «Руководство по установке и настройке»;

## 1.2 Назначение системы

СКФВТ предназначена для контентной фильтрации и антивирусной защиты веб-трафика, а также выполнения функций по разграничению доступа пользователей к внешним веб-ресурсам сети Интернет. СКФВТ обеспечивает отказоустойчивый и контролируемый доступа в сеть Интернет корпоративных пользователей.

К основным функциональным возможностям СКФВТ относятся:

- Разграничение доступа пользователей к ресурсам сети интернет;
- Категорирование веб ресурсов на основе тематики ресурса;
- Фильтрации вредоносного ПО при загрузке файлов с ресурсов сети интернет;
- Предоставление статистической информации по работе пользователей с интернет ресурсами.

# 2 Условия применения

## 2.1 Требования к аппаратному обеспечению

АРМ администратора, с которого будет выполняться подключение к узлам фильтрации СКФВТ, должно соответствовать характеристикам не ниже следующих:

- CPU: 1 процессор с тактовой частотой 1,4 ГГц;
- RAM: 4 Гб;
- HDD: 60 Гб;
- 1 сетевой Ethernet интерфейс с пропускной способностью 100 Мбит/с.

## 2.2 Требования к программному обеспечению

На АРМ администратора, с которого будет выполняться подключение к модулям СКФВТ, должно быть установлено следующее ПО:

- ОС Windows 7/10;
- веб-обозреватель Internet Explorer версии 10 и выше;
- Putty или аналогичный SSH-клиент.

## 2.3 Требования к уровню подготовки обслуживающего персонала

Администратор СКФВТ должен обладать следующими знаниями:

- понимание принципов работы протоколов стека TCP/IP;
- понимание принципов функционирования протоколов HTTP, HTTPS, FTP и SSH;
- понимание принципов функционирования средств проксирования трафика;
- навыки администрирования ОС Red Hat Enterprise Linux.

Перед началом работы с СКФВТ администратор должен ознакомиться с настоящей инструкцией и проектной документацией.

# 3 Обслуживание системы

## 3.1 Общая информация

### 3.1.1 Доступ к интерфейсу администратора

Для входа в интерфейс администратора системы необходимо использовать веб-интерфейс системы, для чего необходимо воспользоваться веб браузером и осуществить подключение к системе по ссылке http://<ip>, где <ip> это назначенный ip адрес сетевой карты сервера. Доступ к системе также возможен по FQDN имени, например http://surfsecue.domain.local, если данное имя задано в корпоративном DNS сервере.

Доступ к веб интерфейсу системы должен осуществляться без использования прокси сервера.

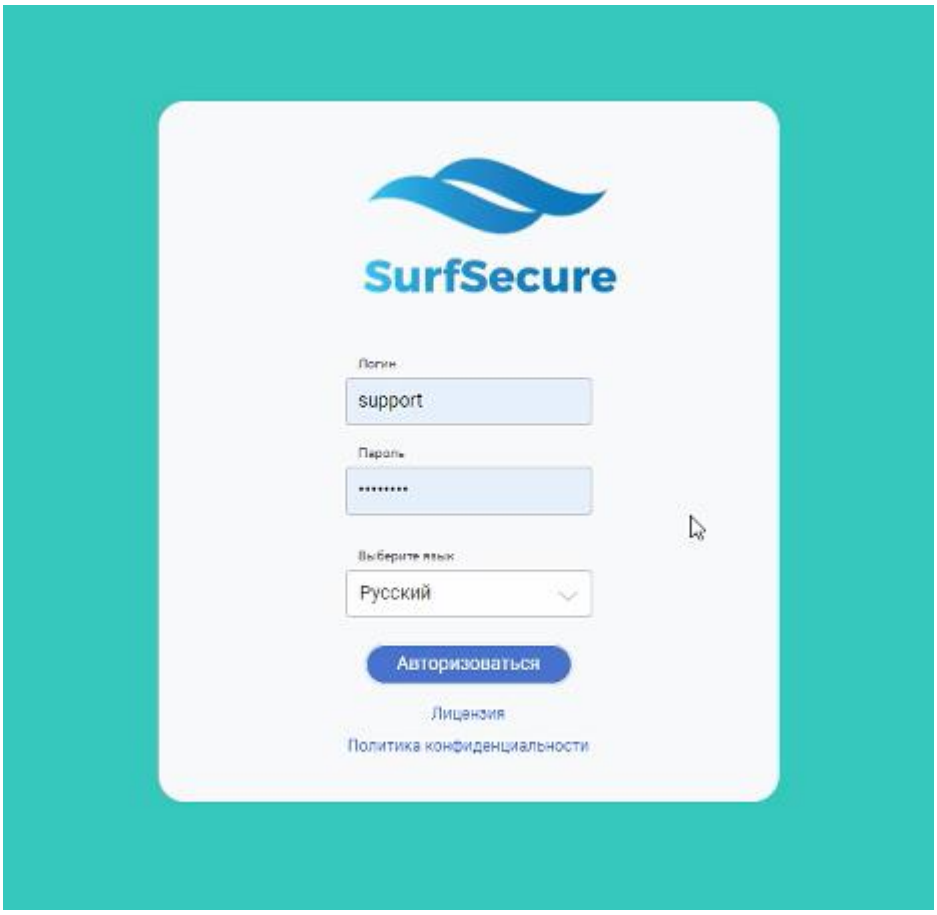


Рисунок 1 – Окно авторизации веб интерфейса системы

Для первичного входа в интерфейс необходимо воспользоваться встроенной учётной записью:

- Логин – support;
- Пароль – password.

Далее необходимо нажать кнопку «Авторизоваться», что приведёт к переходу к меню обзора состояния системы (Рисунок 2).

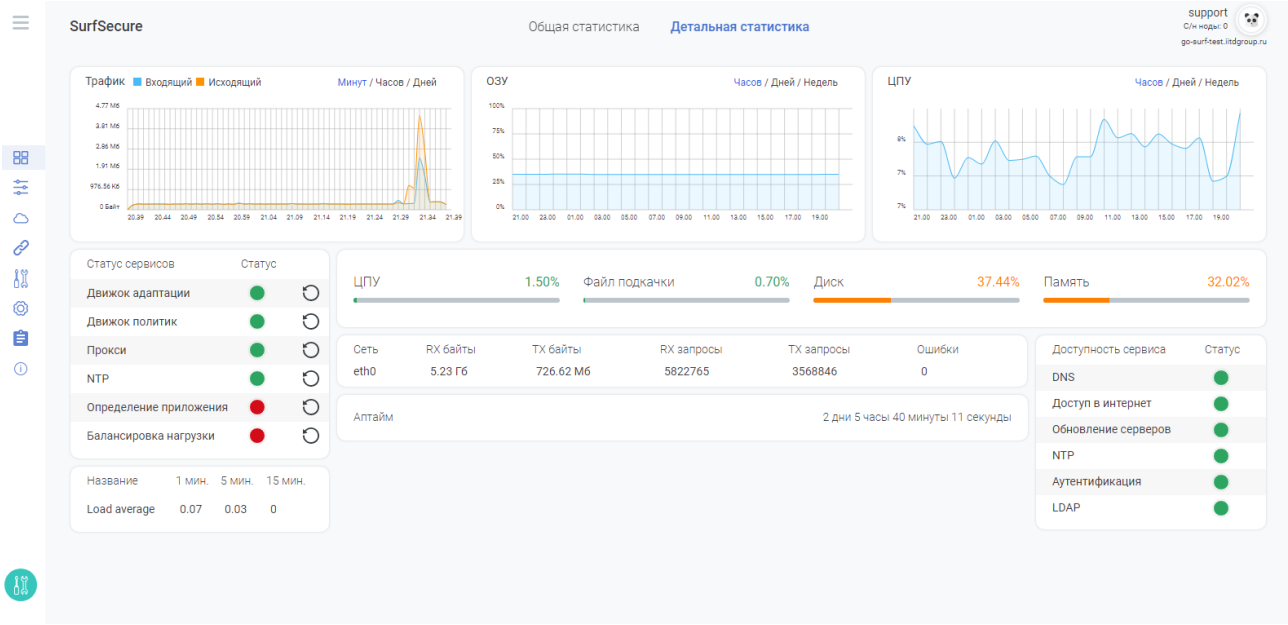


Рисунок 2 – Окно состояния системы

В левой части интерфейса представлены пиктограммы разделов для конфигурации параметров работы системы. Для раскрытия перечня разделов необходимо нажать на пиктограмму , после чего будет отображён перечень разделов (Рисунок 3). Данное меню является основным для навигации и настроек параметров системы.

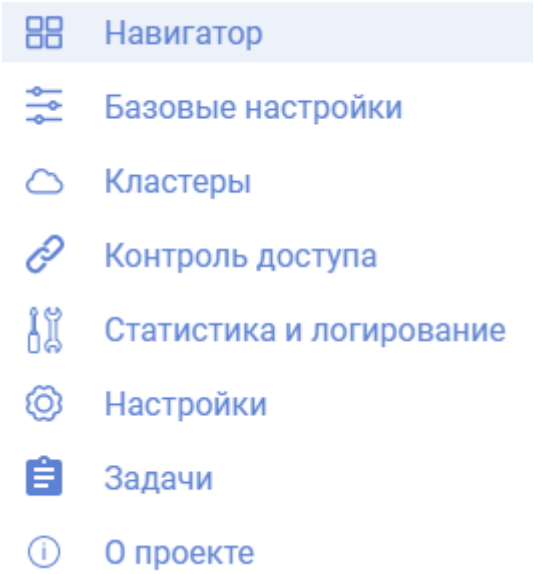


Рисунок 3 – Разделы конфигурирования настроек системы

В верхней правой части отображено имя учётной записи и доменное имя системы (Рисунок 4). Для доступа в раздел персональных настроек необходимо нажать на данную область, после чего отобразится дополнительное меню.

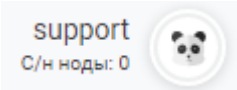


Рисунок 4 – Раздел персональных настроек.

В разделе персональных настроек возможно конфигурирование следующих параметров:

- Theme – цветовое оформление интерфейса системы;
- Interface language – язык веб интерфейса;
- Logout – выход из текущей сессии администратора.

### 3.1.2 Инструменты управления

Веб интерфейс содержит ряд визуальных пиктограмм для работы с настройками системы:

- - Добавление нового параметра;
- - Корректировка заданного значения параметра;
- - Удаление значения\параметра;
- - Закрепить окно интерфейса;
- - Поиск информации;
- - Копирование информации;
- - Сортировка информации.

После внесения изменений в параметры работы системы в обязательном порядке требуется применение изменений. Для этого в левом нижнем углу системы необходимо нажать на пиктограмму и во всплывающем меню подтвердить внесение изменений. Если данное действие не было выполнено, то после перезагрузки системы или несовместимости некоторых настроек – все проведённые изменения будут утеряны.

Выключение и перезагрузка узла фильтрации осуществляются штатными средствами управления, которые располагаются в разделе «Базовые настройки системы», в модуле «Обслуживание» (см. п.3.3.6).

## 3.2 Информация о состоянии системы

Для просмотра статистической информации по работе системы и статуса работы вспомогательных служб необходимо перейти в левой части меню в раздел «Навигатор» (Рисунок 5).

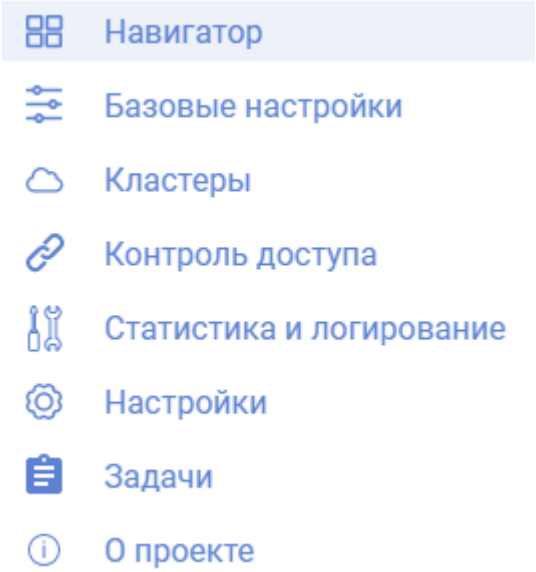


Рисунок 5 – Раздел «Навигатор» в меню навигации

Раздел «Навигатор» имеет два основных меню:

- Общая статистика;
- Детальная статистика.

### 3.2.1 Общая статистика

Меню «Общая статистика» (Рисунок 6) отражает суммарную статистическую информацию по обработанному пользовательскому трафику без учета служебных запросов (обращения к каталогу доменов, обновление антивирусных баз данных и т.д.).

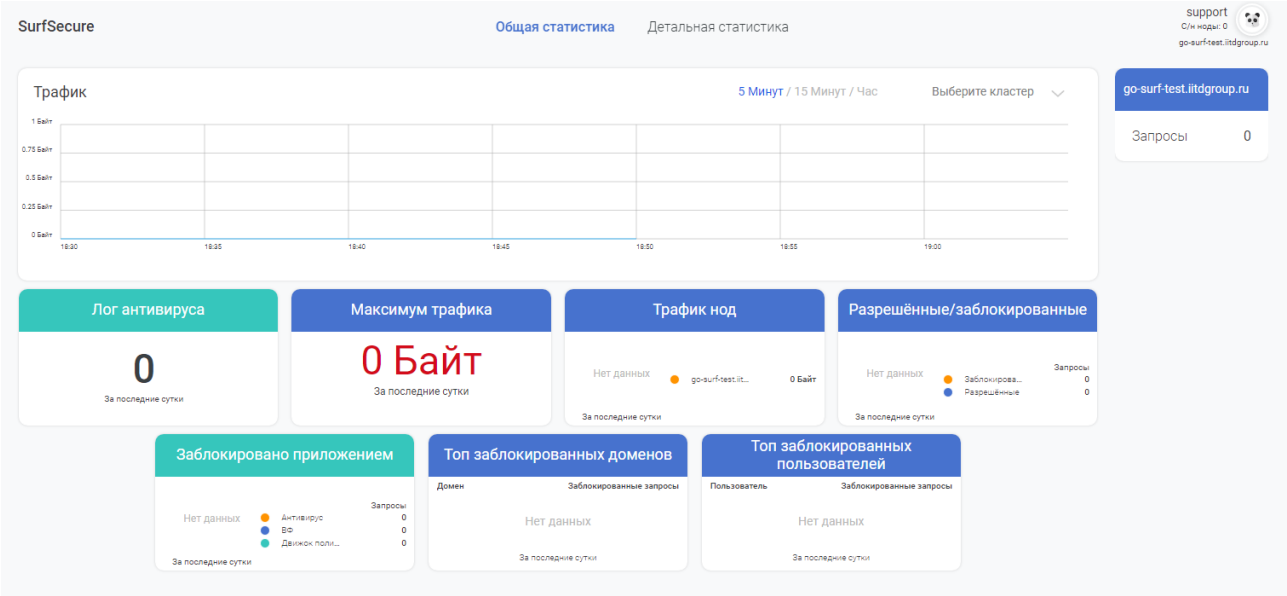


Рисунок 6 – Меню «Общая статистика»

Меню «Общая статистика» содержит следующие модули:

- Трафик – отображает общее количество трафика, обработанное системой за выбранный промежуток времени, за выбранный интервал времени с отображением информации по каждому узлу фильтрации. Модуль имеет возможность выбора следующих параметров:
    - Интервала времени:
        - Последние 5 минут;
        - Последний 15 минут;
        - Последний час.
    - Кластера – если система содержит несколько кластеров распределения нагрузки, возможно отображение информации по каждому кластеру отдельно.
- Лог антивируса – количество запросов, заблокированных антивирусным механизмом, за последний сутки;
- Максимум трафика – суммарное количество трафика, обработанное за последние сутки;
- Трафик нод – количество трафика, обработанное каждым узлом фильтрации, за последние сутки;
- Разрешенные\заблокированные – сводная информация по количеству разрешенных и заблокированных запросов пользователей за последние сутки;
- Заблокировано приложением – сводная информация по количеству заблокированных запросов пользователей за последние сутки с распределением по механизмам блокировки (антивирус, политики и т.д.);
- Топ заблокированных доменов – сводная информация за последние сутки по наиболее популярным доменам, доступ к которым был заблокирован;
- Топ заблокированных пользователей – сводная информация за последние сутки по пользователям, для которых было выявлено максимальное количество заблокированных запросов.

Все модули, за исключением модуля «Трафик», имеют возможность отображения детальной информации. Для этого необходимо нажать на область данного модуля, после чего откроется дополнительное окно (

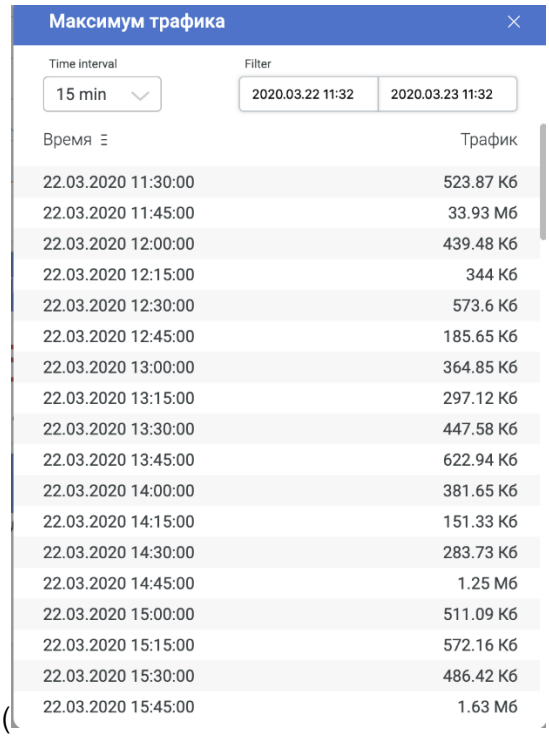


Рисунок 7) с возможностью выбора дополнительных параметров:

- Time interval – временной интервал, за который будет отображена суммарная численная статистика выбранного параметра;
- Filter – временной промежуток, за который будет представлена выборка статистической информации по просматриваемой информации.

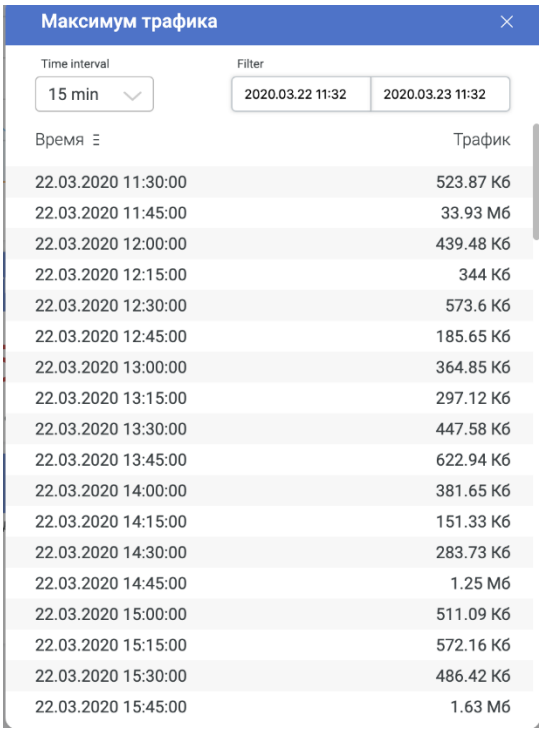


Рисунок 7 – Окно детального информации модуля «Максимум трафика»

В правой части интерфейса общей статистики отображается информация о подключенных узлах фильтрации и количеству обработанных запросов пользователей за последние сутки (Рисунок 8).

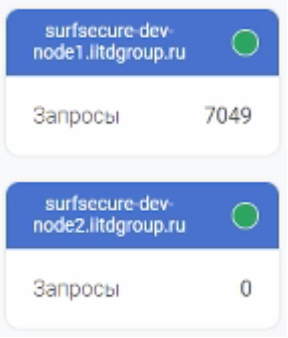


Рисунок 8 – Перечень узлов фильтрации

После нажатия в область нужного узла фильтрации будет отображена детальная информация по работе выбранного узла фильтрации (Рисунок 9), аналогично меню «Детальная статистика» (см. пункт 3.2.2) за исключением статуса взаимодействия со смежными системами (доменный каталог пользователей, DLP сервер и т.д.).

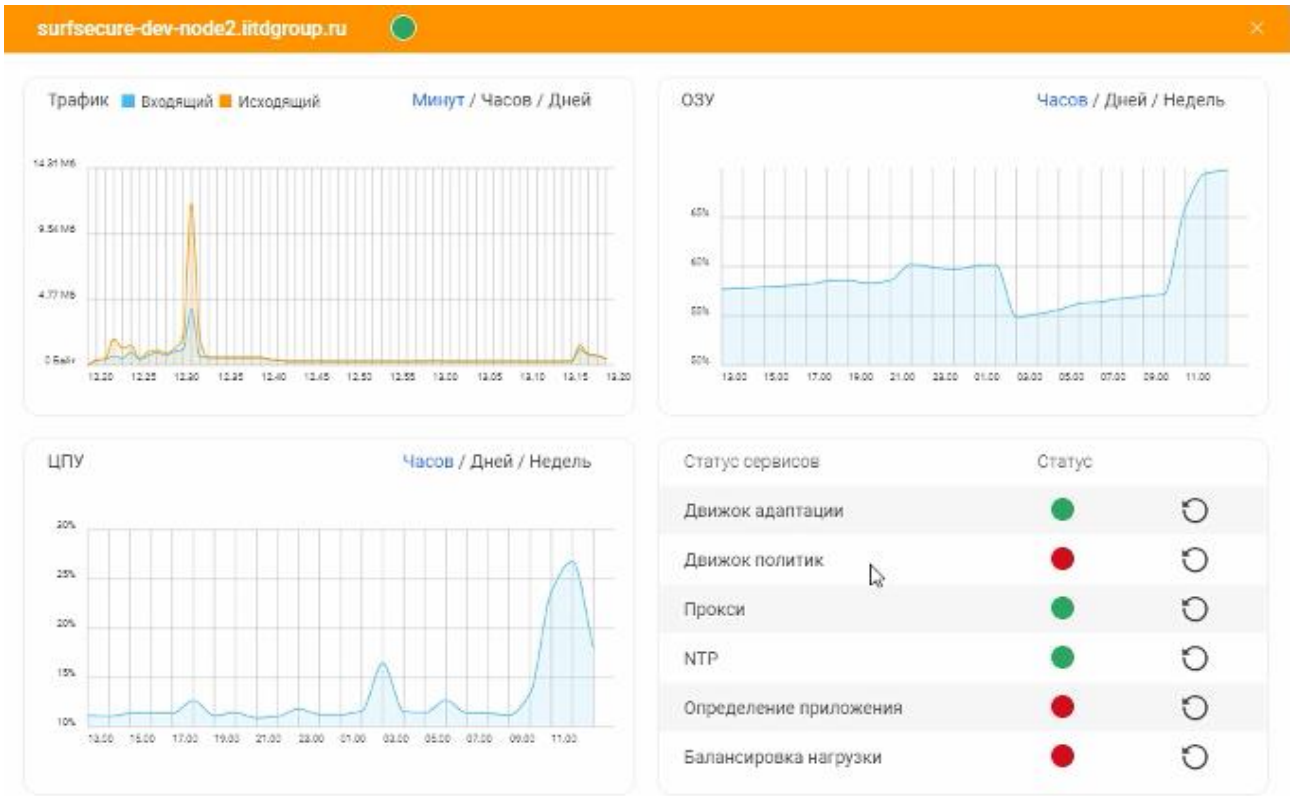


Рисунок 9 – Детальная статистика работы узла фильтрации

### 3.2.2 Детальная статистика

Меню «Детальная статистика» (Рисунок 10) отображает подробные параметры работы узла фильтрации и функционирования его служебных модулей. Данное меню отображает информацию только по тому узлу фильтрации, к которому была открыта текущая сессия в веб интерфейс администратора. Для просмотра детальной статистики других узлов необходимо

перейти в меню «Общая статистика» и выбрать необходимый узел фильтрации (см. пункт 3.2.1).

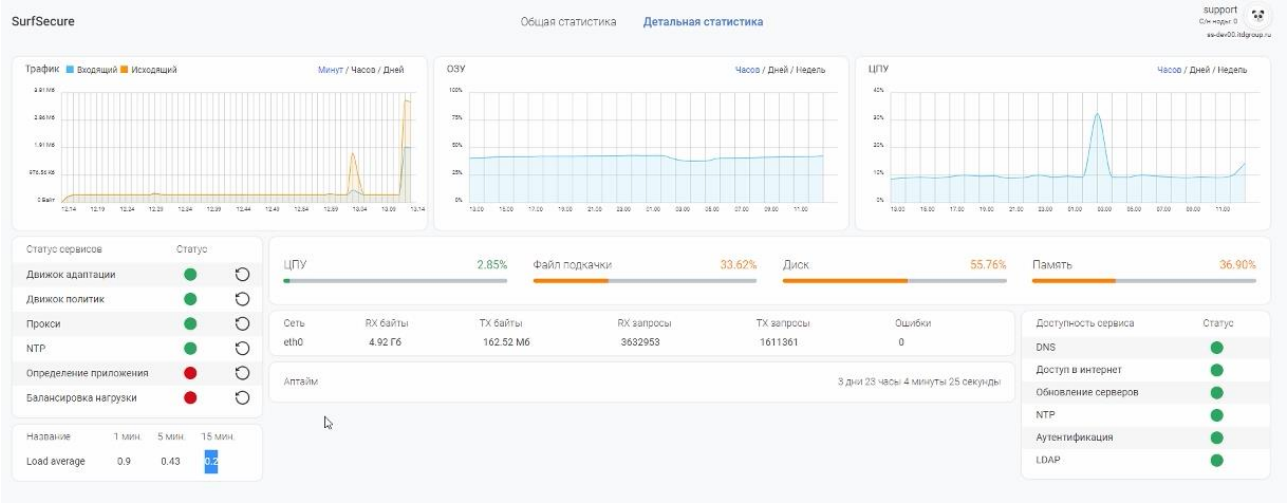


Рисунок 10 – Меню «Детальная статистика»

Интерфейс детальной статистики работы узла фильтрации содержит следующие модули:

- Трафик – количество исходящего и входящего трафика, обработанного узлом фильтрации, в т.ч. служебного, за выбранный промежуток времени;
- ОЗУ – статистика использования оперативной памяти за выбранный промежуток времени;
- ЦПУ - статистика загрузки процессора за выбранный промежуток времени;
- Статус сервисов – отображает статус работы внутренних служб. С помощью пиктограммы возможно принудительно инициировать перезагрузку сервиса;
- Доступность сервиса – отображает статус доступности внешних сервисов;
- Аптайм – время работы узла фильтрации с момента последнего запуска;
- Сеть - сводная информация по обработке сетевого трафика с разделением на каждый сетевой интерфейс узла фильтрации;
- Load average – средняя загрузка узла фильтрации за предопределенные интервалы времени.

В центральной части представлена информация о текущей загрузке системы в реальном времени (Рисунок 11).


Рисунок 11 – Информация о текущей загрузке узла фильтрации

## 3.3 Базовые настройки системы

Раздел базовых настроек системы предназначен для установки или изменения параметров, которые необходимы для корректной работы самого узла фильтрации. Для

конфигурирования данных параметров необходимо выполнить переход в раздел «Базовые настройки» и далее выбрать меню «Системные настройки» (Рисунок 12).

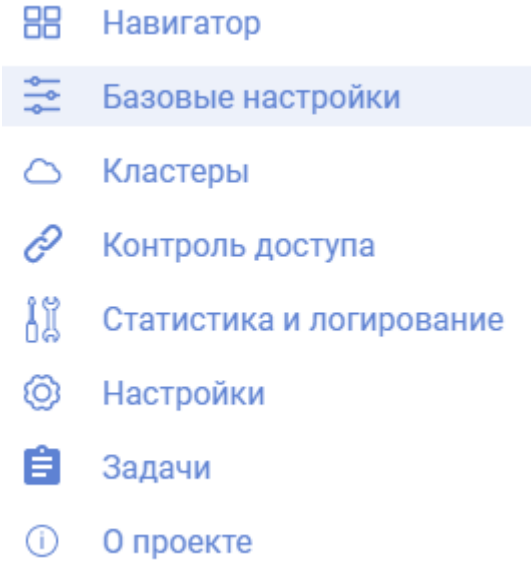


Рисунок 12 – Раздел «Базовые настройки» в меню навигации

Интерфейс меню системных настроек представлен ниже (Рисунок 13).

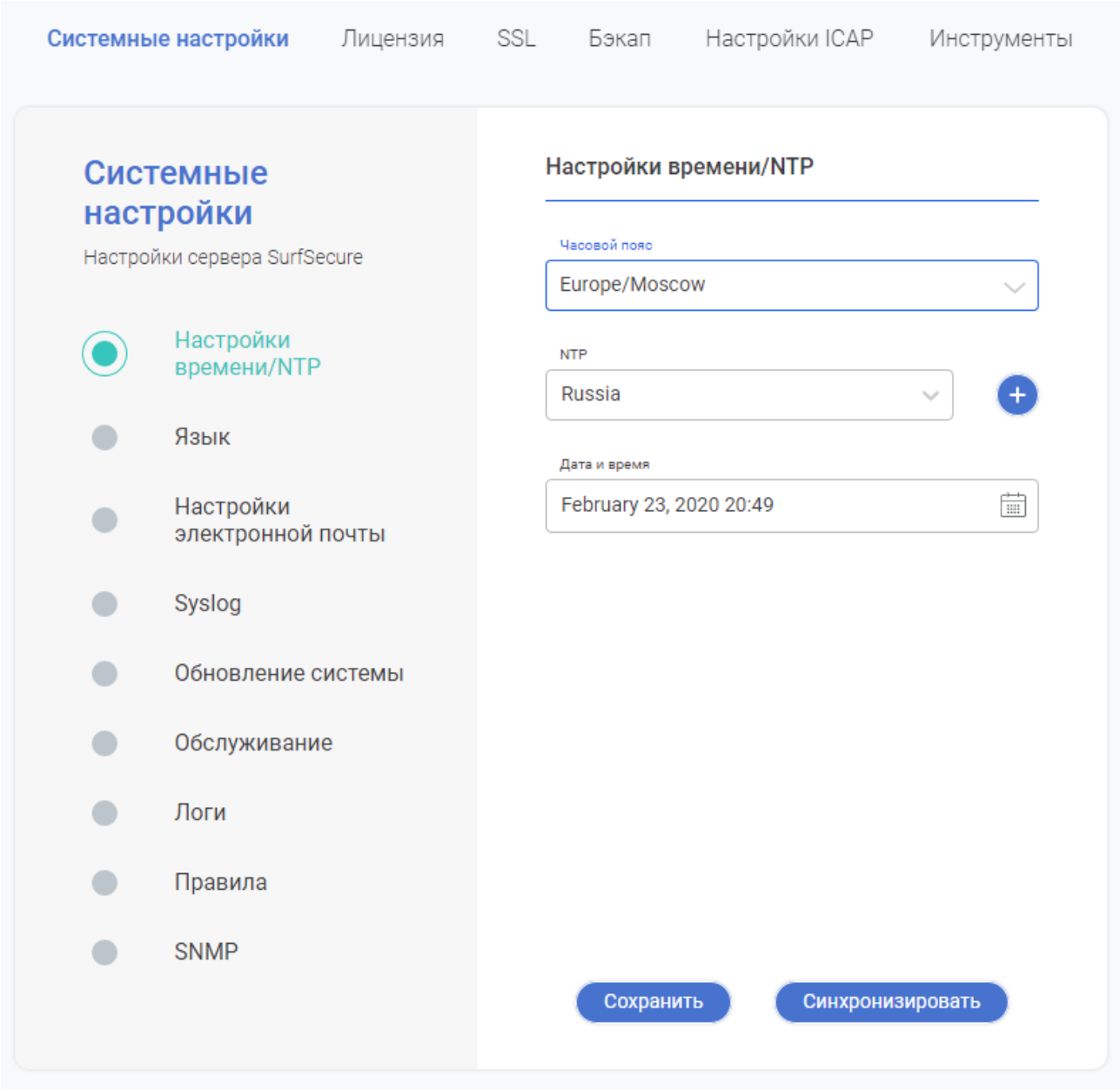


Рисунок 13 – Меню системных настроек

Меню «Системные настройки» содержат следующие модули для конфигурации параметров работы системы:

- Настройки времени/NTP – конфигурирование настроек времени системы и\или использования внешнего NTP сервера;
- Язык – выбор языка для отображаемых оповещений и ошибок системы;
- Настройки электронной почты – настройка параметров оповещения по электронной почте;
- Syslog – настройка параметров логирования;
- Обновление системы – выполнение действий по обновлению используемой версии ПО узла фильтрации;
- Обслуживание – выключение или перезапуск системы;
- Логи – выгрузка логов системы и включение режима отладки;

- Правила – установка параметров обработки списков правил и действия по умолчанию;
- SNMP – настройка параметров для подключения внешнего сервиса мониторинга.

### 3.3.1 Настройка времени

Интерфейс настройки временных параметров представлен ниже (Рисунок 14).

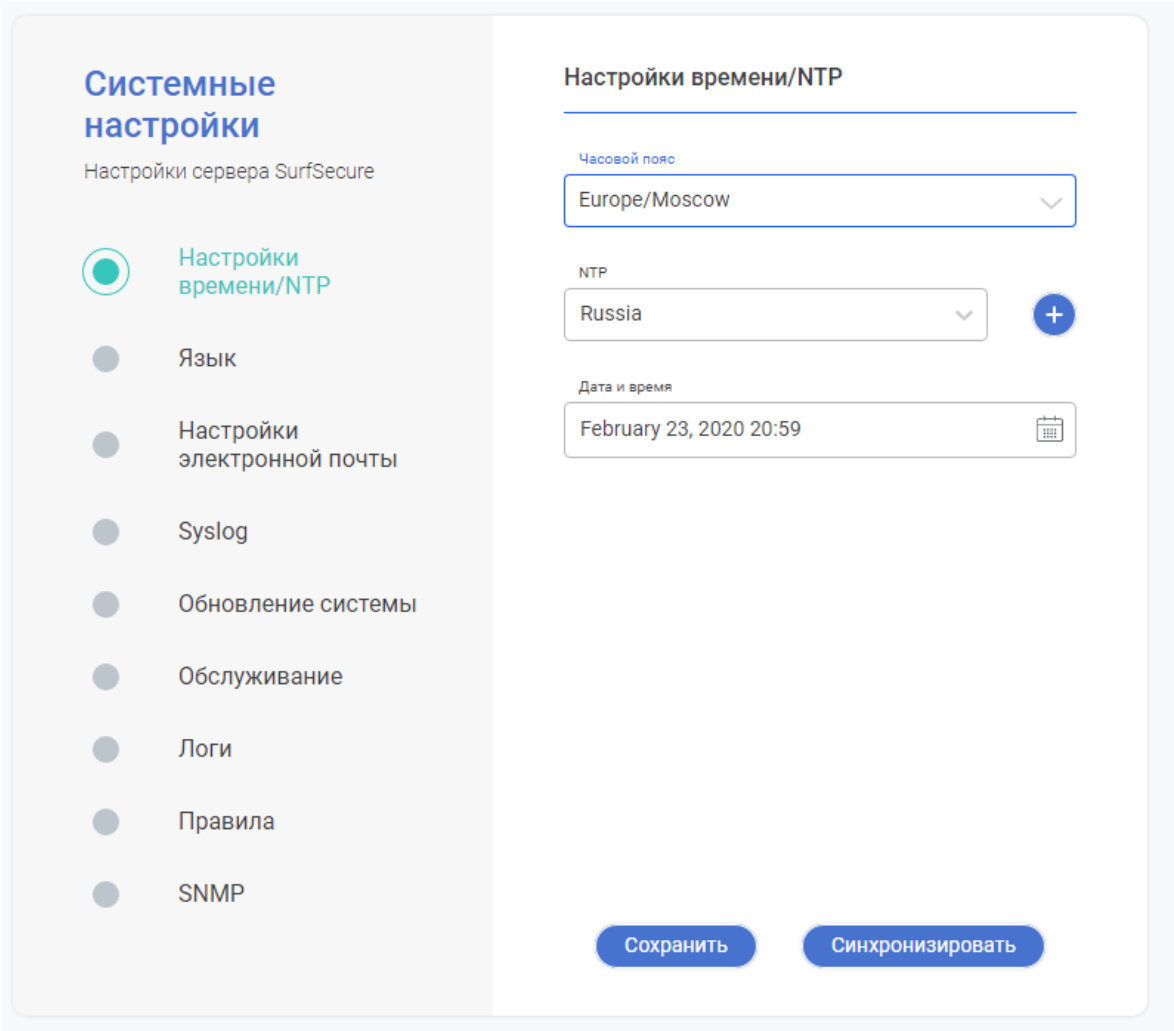


Рисунок 14 – Интерфейс настройки параметров времени

Для корректной работы системы в обязательном порядке требуется указание правильного системного времени и часового пояса. Данную операцию можно выполнить двумя способами:

- Интеграция с NTP сервером (рекомендуется производителем);
- Установка времени в ручном режиме (используется только в случае отсутствия доступа ко внутреннему или внешнему NTP серверу).

Вне зависимости от выбора варианта настройки требуется указать верный часовой пояс системы, для этого из выпадающего списка «Часовой пояс» необходимо выбрать

часовой пояс, в котором расположен узел фильтрации, из списка, предустановленного производителем.

В случае отсутствия корпоративного NTP сервера, производителем предусмотрен перечень внешних общедоступных NTP сервисов. Из выпадающего списка «NTP» необходимо выбрать NTP сервер, который находится в наибольшей близости к месту установки узла фильтрации (для России – необходимо выбрать NTP сервер Russia). Далее необходимо нажать кнопку «Сохранить», после сохранения настроек нажать кнопку «Синхронизировать» и убедиться, что в поле «Дата и время» отражены корректные данные.

Для настройки интеграции с корпоративным NTP сервером необходимо его добавить в список путем нажатия пиктограммы + и указания его наименования и IP адреса. Далее необходимо подтвердить корректность указания данных нажатием пиктограммы OK и выбрать добавленный NTP сервер из выпадающего списка (находится в конце списка). Далее необходимо нажать кнопку «Сохранить», после сохранения настроек нажать кнопку «Синхронизировать» и убедиться, что в поле «Дата и время» отражены корректные данные.

Установка времени в ручной режиме осуществляется путем ручного указания текущей даты и времени в соответствующем поле и нажатием кнопки «Сохранить».

### 3.3.2 Язык

Интерфейс настройки языковых параметров представлен ниже (Рисунок 15).

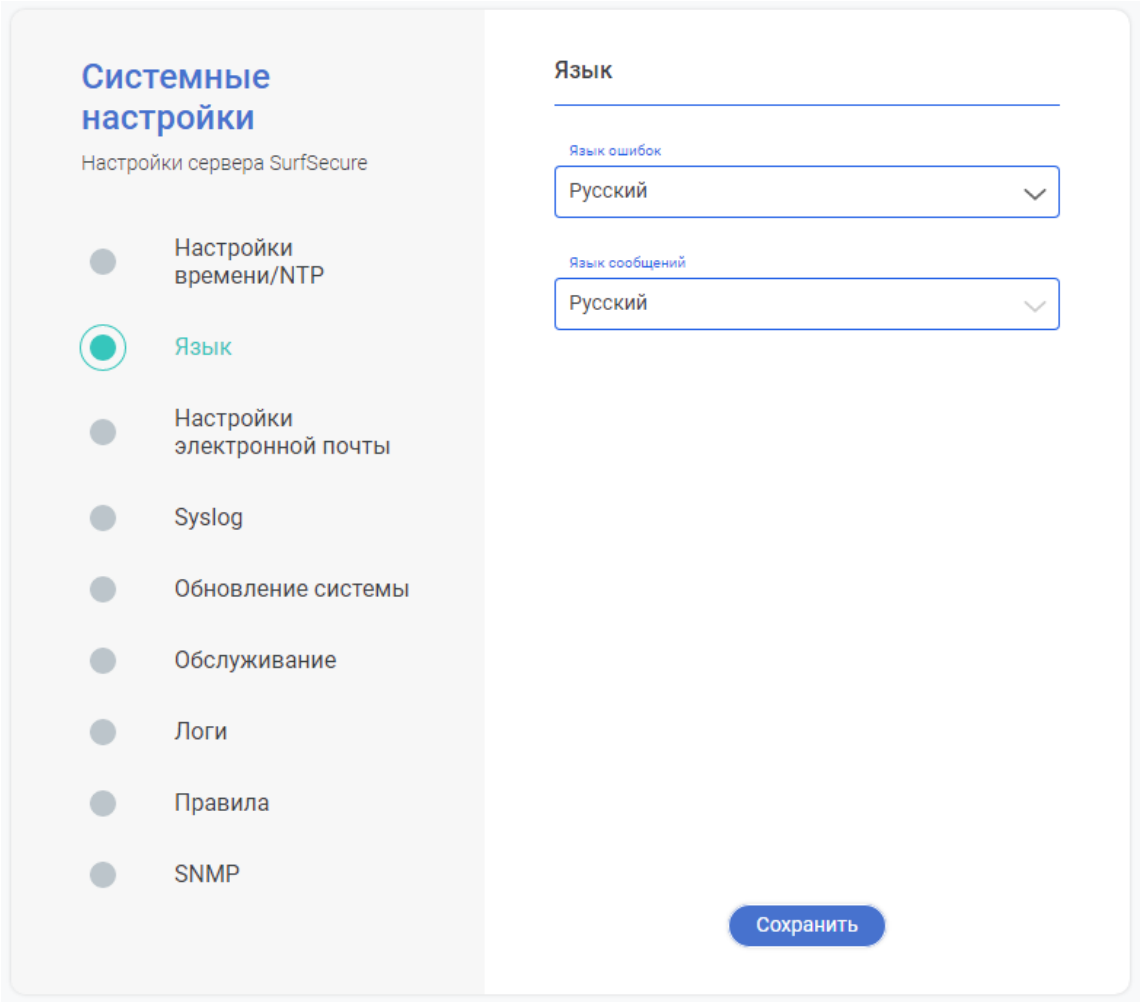


Рисунок 15 – Модуль настройки языковых параметров

В данном разделе существует возможность настроить следующие параметры:

- Язык ошибок – настройка языковых параметров сообщений об ошибках, выдаваемых системой;
- Язык сообщений – настройка языковых параметров, которые будут использоваться при построении отчетов о работе системы в разделе «Статистика и логирование».

Для задания языковых параметров необходимо из выпадающего списка выбрать требуемый язык и нажать кнопку «Сохранить».

### 3.3.3 Настройка электронной почты

Данные параметры необходимы для настройки почтовых оповещений администратора системы об изменениях параметров состояния системы, например ошибка обновления антивирусного механизма. Интерфейс настройки языковых параметров представлен ниже (Рисунок 16).

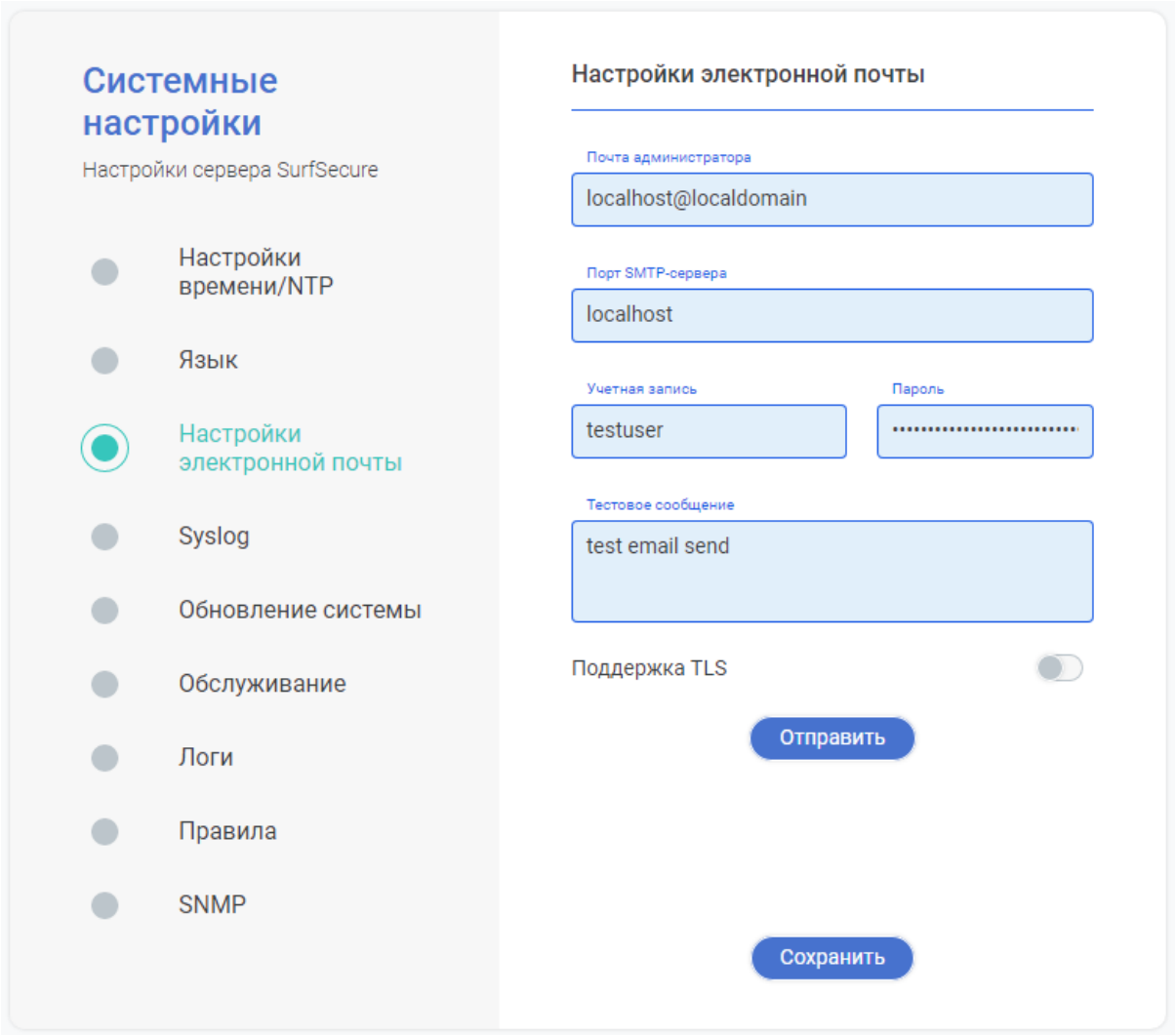


Рисунок 16 – Интерфейс конфигурирования параметров оповещения администратора

Для настройки параметров почтового оповещения администраторов системы необходимо указать следующие параметры:

- Почта администратора – почтовый адрес администратора или группы рассылки;
- Порт SMTP-сервера – IP адрес корпоративного почтового сервера, по умолчанию используется 25-ый порт для подключения к SMTP серверу. Если требуется указать нестандартный порт для подключения к почтовому серверу по протоколу SMTP, в таком случае необходимо указать его через двоеточие в формате <IP адрес>:<порт>;
- Учетная запись и пароль – если почтовый сервер требует принудительной аутентификации, то в данных полях необходимо указать информацию об учетной записи для интеграции;
- Поддержка TLS – данную функцию необходимо включить в случае, если для взаимодействия с почтовым сервером требуется защищенное соединение.

После ввода вышеуказанных параметров необходимо нажать кнопку «Сохранить». Для проверки корректности интеграции возможно задействовать встроенный функционал отправки тестового сообщения – для этого в поле «Тестовое сообщение» ввести

произвольный текст и нажать кнопку «Отправить» для отправки пробного сообщения. Результат отправки будет отображен в текстовом виде.

### 3.3.4 Syslog

Данный механизм обеспечивает регистрацию запросов пользователей и результатов их обработки в формате syslog. Интерфейс настроек Syslog представлен ниже (Рисунок 17).

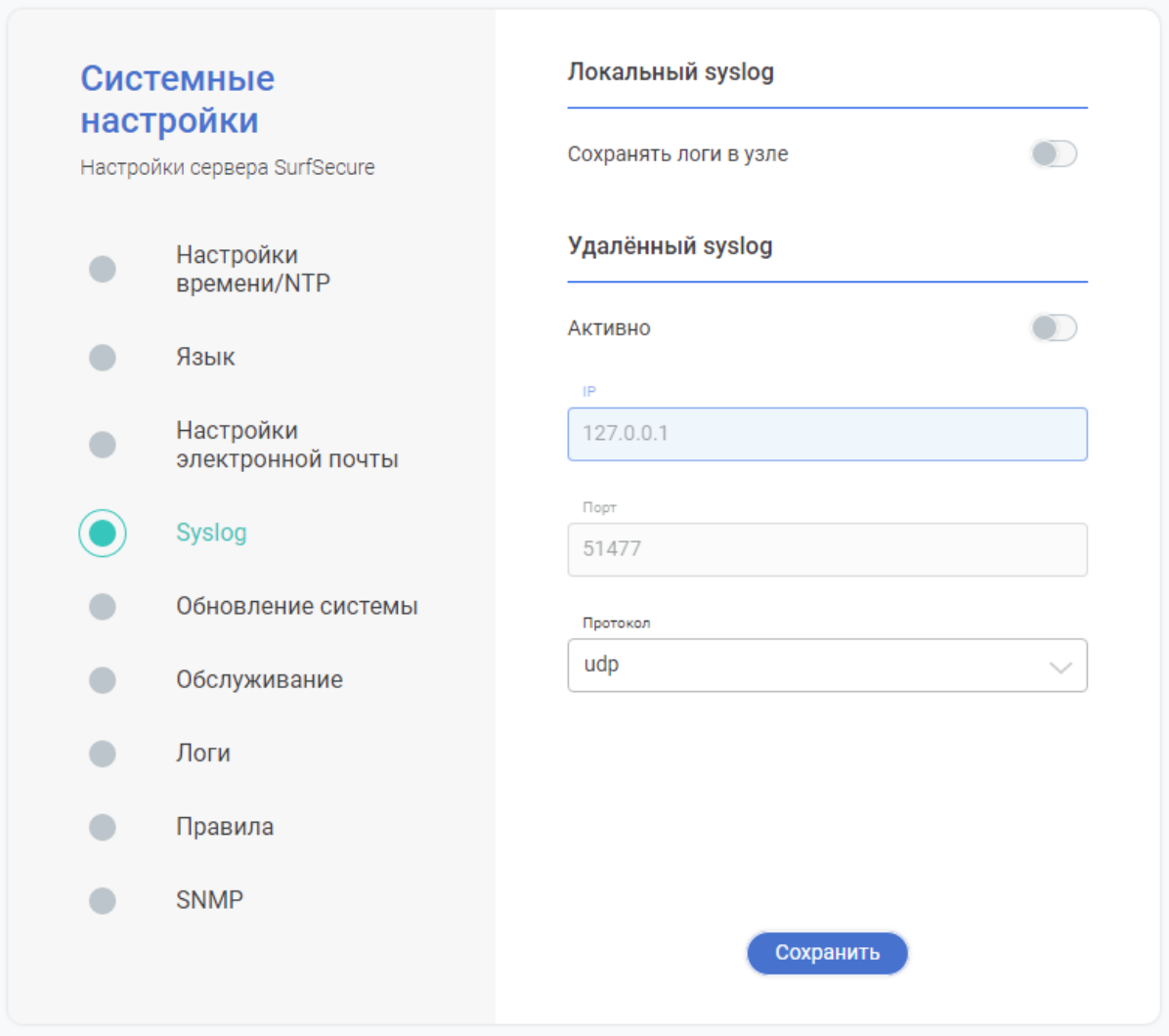


Рисунок 17 – Интерфейс конфигурирования параметров syslog

Система по умолчанию регистрирует данные события в отдельной базе данных для формирования отчетности, поэтому механизм syslog следует рассматривать как дополнительный инструмент по регистрации событий обработки трафика. Система позволяет использовать механизм Syslog в следующих режимах:

- Локальный – все события будут записывать в файл, хранящийся локально на узле фильтрации;
- Удаленный – все события будет отправляться в корпоративный syslog сервер. Для этого необходимо указать следующие параметры:
    - IP адрес syslog сервера;
    - Порт;

- Протокол взаимодействия.

Вышеуказанные режимы работы не являются взаимоисключающими и могут быть включены одновременно. По окончанию настройки необходимо нажать кнопку «Сохранить».

### 3.3.5 Обновление системы

Данный интерфейс (Рисунок 18) предназначен для проверки актуальности и обновления версии ПО, используемого узлом фильтрации.

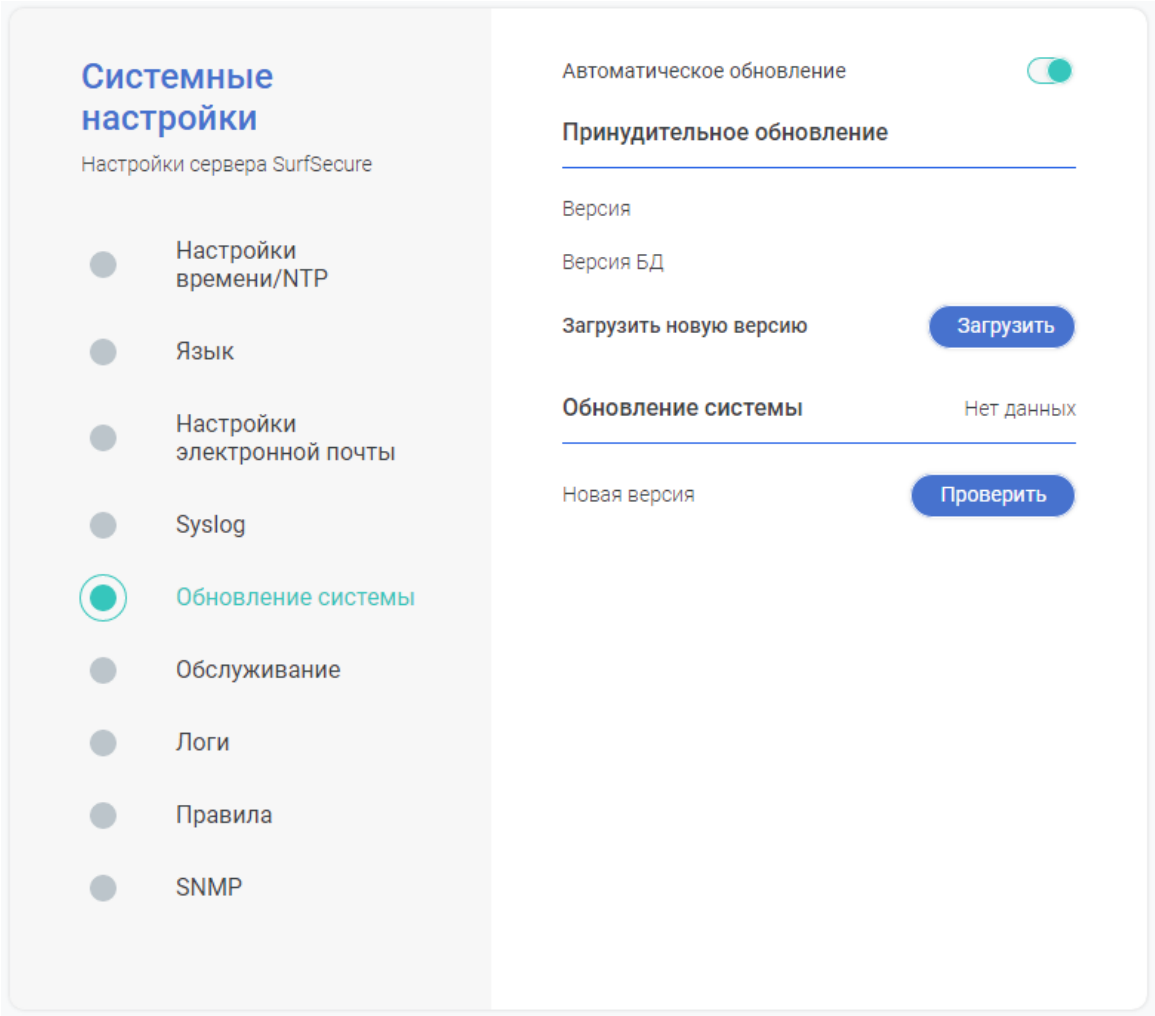


Рисунок 18 – Интерфейс конфигурирования параметров обновления системы

Система имеет встроенный функционал автоматического обновления версии ПО с сайта производителя. Для успешного получения обновлений, системе необходим доступ к ресурсам производителя update.surfsecure.net по портам TCP 80 и 443. По умолчанию данный функционал включен, для его отключения необходимо нажать на пиктограмму .

Существует возможность обновления версии ПО в ручном режиме, для этого предварительно необходимо запросить у производителя файл, содержащий последние обновления системы. Далее в области «Принудительное обновление» необходимо нажать на

кнопку «Загрузить» и выбрать файл-обновление, после чего начнется процесс обновления системы.

Для проверки актуальности используемого ПО необходимо нажать на кнопку «Проверить» в области «Обновление системы». По окончанию проверки система выдаст текстовое уведомление об актуальности используемого ПО или последнюю версию ПО, выпущенным производителем. Если на узле фильтрации используется неактуальная версия ПО, по окончанию проверки кнопка «Проверить» изменится на кнопку «Обновить», нажатие на которую запустит принудительный процесс обновления узла фильтрации на новую версию ПО.

### 3.3.6 Обслуживание

Раздел «Обслуживание» (Рисунок 19) содержит штатные инструменты для выключения или перезапуска узла фильтрации.

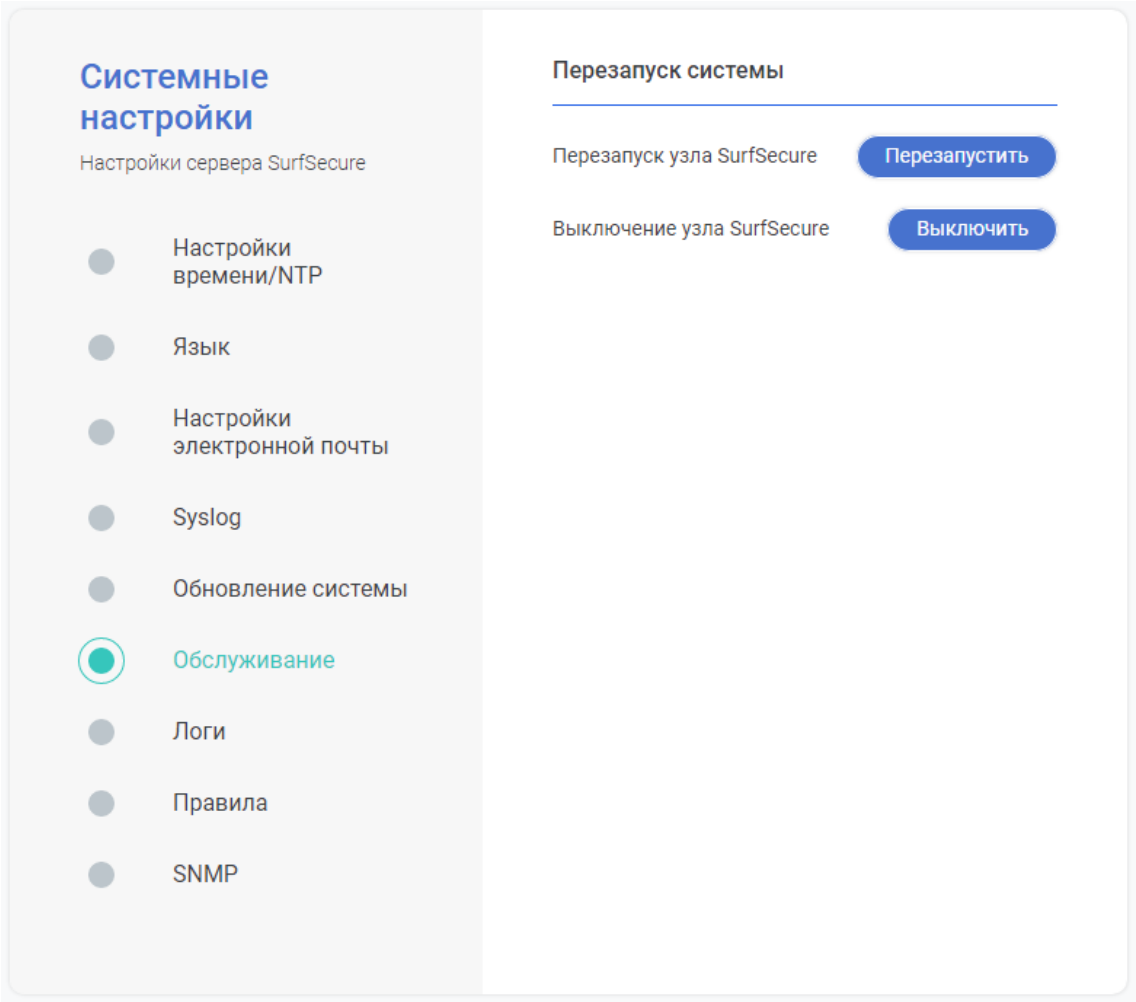


Рисунок 19 – Интерфейс модуля «Обслуживание»

Интерфейс предусматривает выполнения следующие возможности по управлению системой:

- Кнопка «Перезапустить» - выполняет штатный процесс перезапуска узла фильтрации;

- Кнопка «Выключить» - выполняет процесс штатного завершения работы узла фильтрации.

### 3.3.7 Логи

Интерфейс «Логи» (Рисунок 20) предназначен для управления и сбора зарегистрированных событий работы системы для их дальнейшей передачи в службу технической поддержки производителя в случае, если выявлена некорректная работы системы.

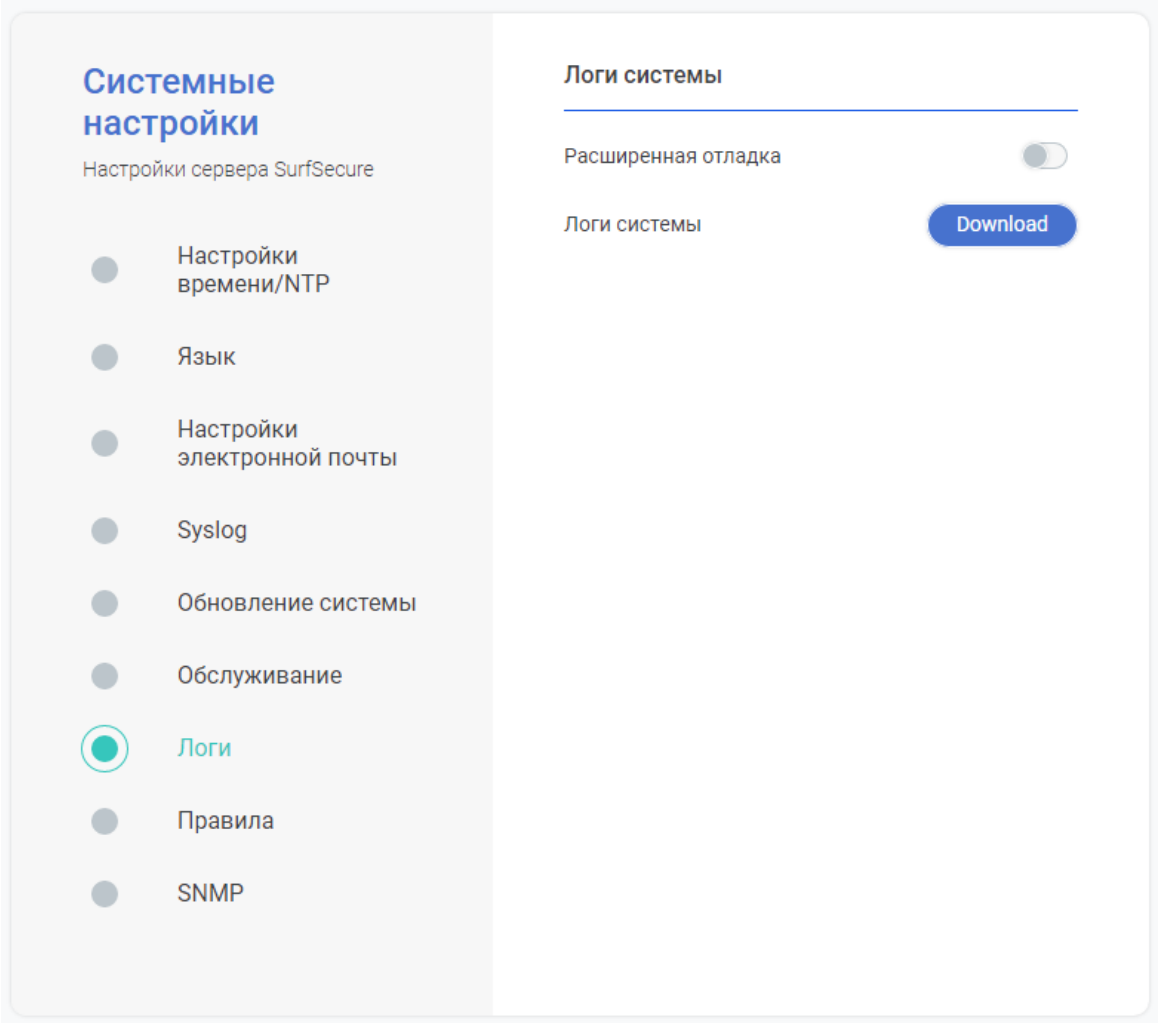


Рисунок 20 – Интерфейс конфигурации настроек параметров логирования

Параметр «Расширенная отладка» включает сохранение информационных сообщений о работе системы в расширенном режиме. Данный параметр необходимо включать только по указанию специалистов технической поддержки производителя, т.к. сбор событий в расширенном режиме оказывает дополнительную нагрузку на вычислительные мощности и может привести к существенной деградации производительности узла фильтрации. При штатной работе узла фильтрации данный параметр должен быть отключен.

Кнопка «Download» позволяет выполнить загрузку собранных сообщений о работе системы на рабочую станцию администратора с целью их дальнейшей передачи специалистам технической поддержки производителя.

### 3.3.8 Правила

Настройки системы в разделе «Правила» (Рисунок 21) позволяют задать действия по умолчанию над пользовательскими запросами, а также определить порядок их обработки.

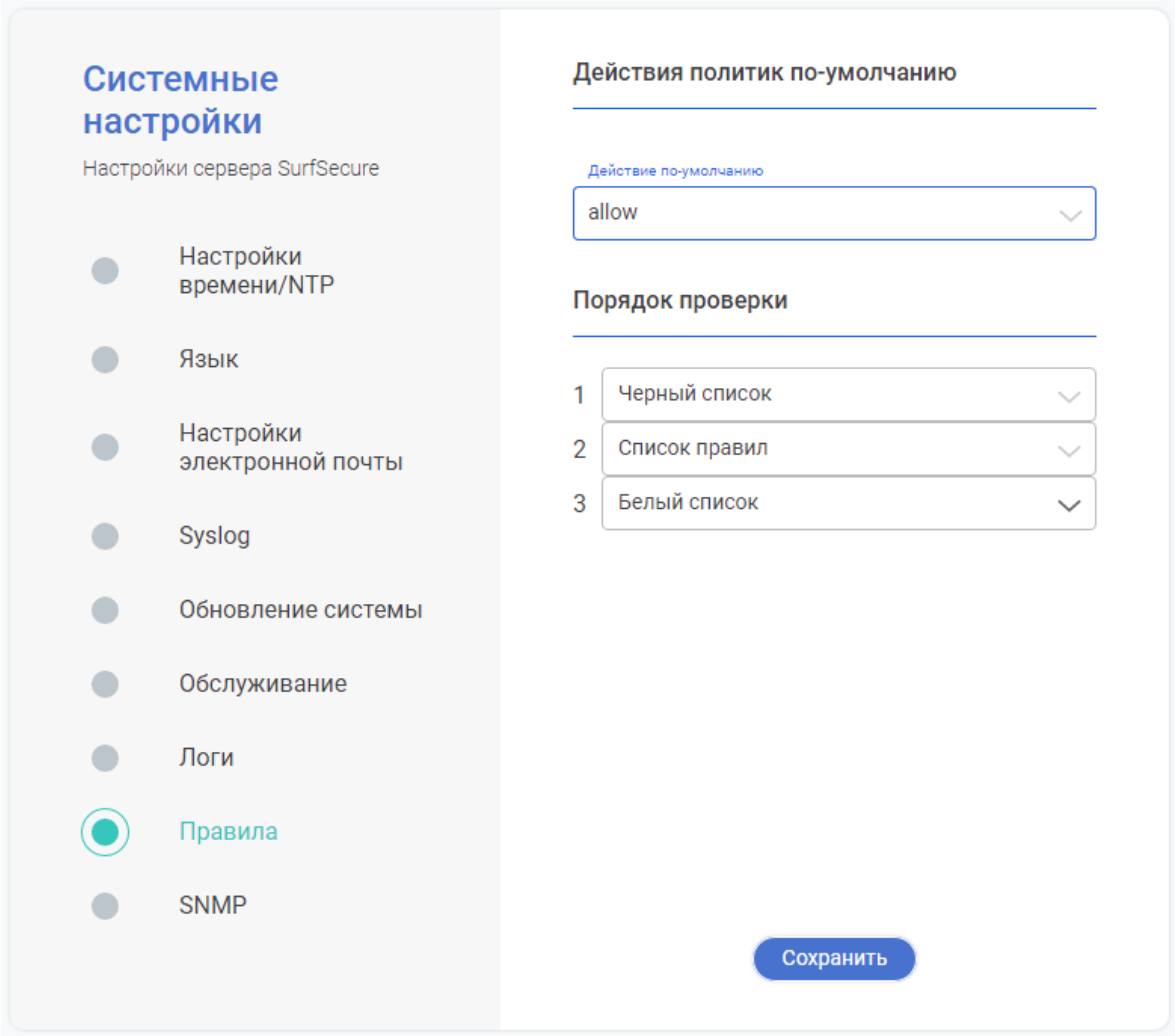


Рисунок 21 – Интерфейс конфигурации базовых параметров обработки трафика

Действие по умолчанию применяется в случае, если пользовательский запрос не попал ни под одно правило, то в таком случае к данному запросу будет также применено действие по умолчанию. Для выбора реакции системы необходимо в выпадающем списке «Действие по умолчанию» выбрать один из двух возможных вариантов:

- Allow – разрешать прохождение запроса;
- Deny – блокировать запрос пользователя.

Также необходимо установить порядок выполнения проверки пользовательских запросов. В процессе фильтрации запроса, система осуществляет проверку на совпадение пользовательского запроса со следующими сущностями:

- Черный список – глобальный перечень веб ресурсов и IP адресов, доступ к которым необходимо заблокировать всем пользователям;
- Белый список - глобальный перечень веб ресурсов и IP адресов, доступ к которым необходимо разрешить всем пользователям;

- Список правил – правила доступа к веб ресурсам, сформированные администратором системы, на основе ряда критериев запроса (принадлежность пользователя к определенной доменной группе, категория запрашиваемого веб ресурса, временной интервал запроса и т.д.).

По окончанию внесения изменений необходимо нажать кнопку «Сохранить».

### 3.3.9 SNMP

Раздел настроек «SNMP» (Рисунок 22) позволяет включить встроенные механизмы для обеспечения контроля состояния узла фильтрации с использованием корпоративной системы мониторинга по протоколу SNMP.

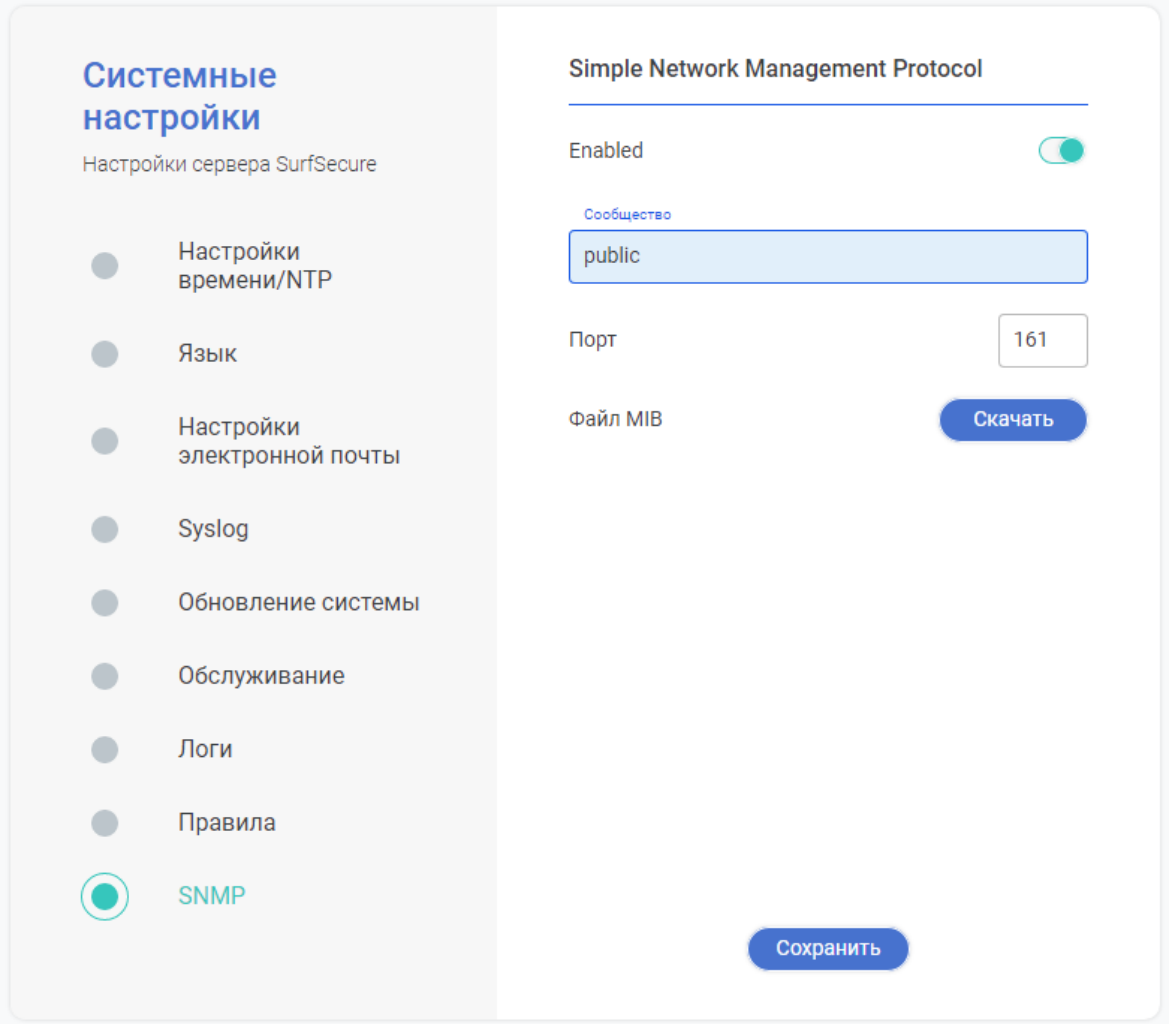


Рисунок 22 – Интерфейс настроек параметров SNMP

По умолчанию, функционал удаленного мониторинга выключен и для его включения необходимо нажать на пиктограмму в строке «Enabled». Следующим шагом нужно указать параметры работы механизма:

- Сообщество – имя для идентификации службы SNMP. Рекомендуется сменить значение по умолчанию «public» в целях безопасности;

- Порт – порт для подключения корпоративной службы мониторинга к узлу фильтрации.

По окончанию изменения параметров необходимо нажать кнопку «Сохранить».

Для упрощения процесса интеграции с корпоративной системой мониторинга, система позволяет выгрузить MIB-файл, который содержит описание параметров системы, с целью его последующего импорта в систему мониторинга. Для выгрузки MIB-файла необходимо нажать кнопку «Скачать», после чего будет начат процесс загрузки файла на рабочую станцию администратора.

## 3.4 Сетевая конфигурация

Интерфейс конфигурации сетевых настроек позволяет управлять параметрами сетевых интерфейсов, настроек разрешение доменных имен, маршрутизации, а также параметрами сетевого доступа к самому узлу фильтрации. Данный интерфейс располагается в разделе «Настройки» в меню «Сеть» (Рисунок 23).

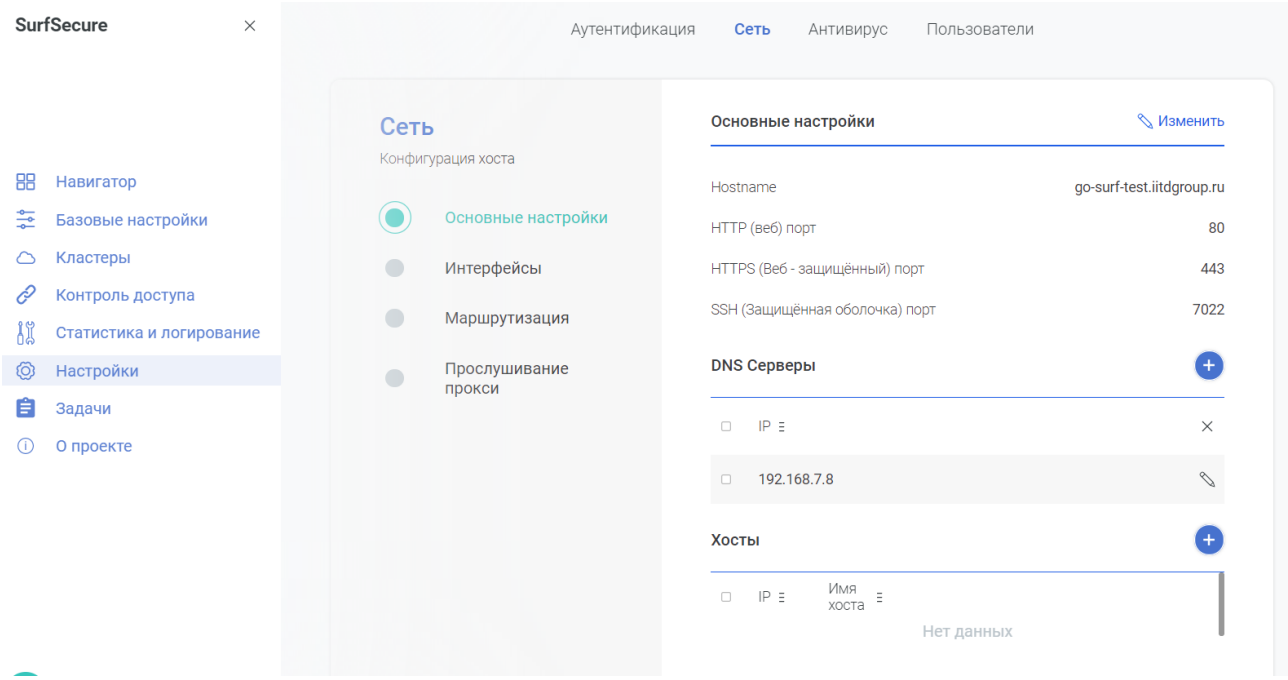


Рисунок 23 – Интерфейс конфигурации основных сетевых настроек

Настройка сетевых параметров узла фильтрации разделена на следующие модули:

- Основные настройки – сетевое имя, параметры доступа, DNS и хост-записи;
- Интерфейсы – параметры сетевых интерфейсов, шлюз по умолчанию;
- Маршрутизация – статические сетевые маршруты;
- Прослушивание прокси – сетевые параметры для подключения пользователей.

### 3.4.1 Основные настройки

В модуле «Основные настройки» (Рисунок 23) возможно корректировать следующие параметры:

- Область «Основные настройки»:

- Hostname – FQDN имя узла фильтрации (изменение данного параметра не рекомендуется, при необходимости изменения следует обратиться в службу технической поддержки производителя);
- HTTP (веб) порт – порт доступа к веб интерфейсу администратора по протоколу HTTP;
- HTTPS (веб – защищенный) порт - порт доступа к веб интерфейсу администратора по протоколу HTTPS;
- SSH (защищенная оболочка) порт - порт доступа к интерфейсу командной строки администратора по протоколу SSH;

Для корректировки данных параметров необходимо нажать кнопку «Изменить» и по окончанию ввода параметров нажать кнопку «Сохранить».

- Область «DNS Серверы» - отображается текущий перечень DNS серверов. Работа с параметрами осуществляется следующими инструментами:
  - для добавления нового DNS сервера;
  - для корректировки IP адреса указанного DNS сервера;
  - для удаления указанного DNS сервера.
- Область «Хосты» - позволяет задать ручную связку IP адреса и DNS имени, которая будет использоваться до обращения к DNS серверу. Работа с параметрами осуществляется следующими инструментами:
  - для добавления нового записи;
  - для удаления записи.

### 3.4.2 Интерфейсы

В модуле «Интерфейсы» отображается текущий перечень настроенных сетевых интерфейсов, их параметры, а также используемый маршрут по умолчанию (Рисунок 24).

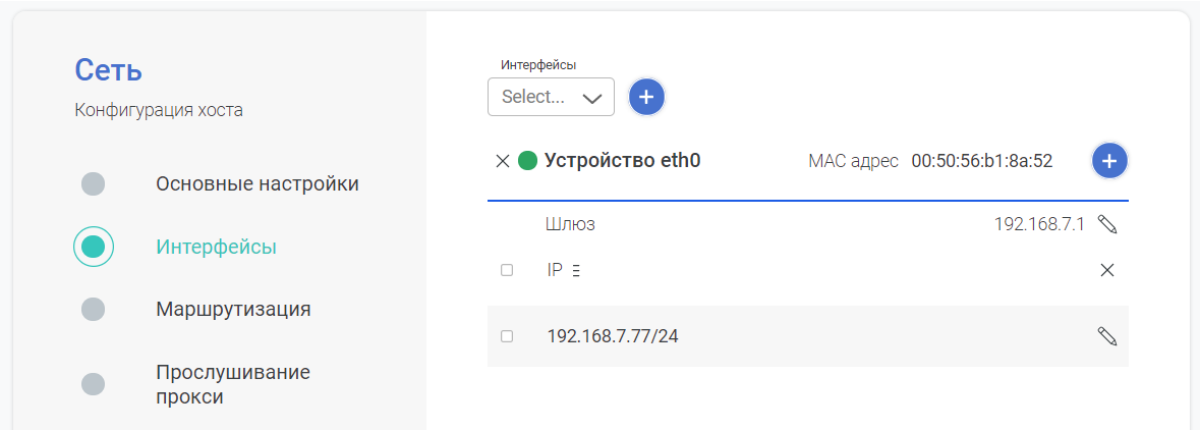


Рисунок 24 – Конфигурация параметров сетевых интерфейсов

Для добавления нового сетевого интерфейса, который присутствует в сервере, но еще не настроен, необходимо выбрать его из выпадающего списка «Интерфейсы» и нажать на

рядом стоящую пиктограмму , после чего новые интерфейс отобразится в основной области интерфейса. Добавление основного или создание дополнительного IP адреса на интерфейсе осуществляется путем нажатия на пиктограмму напротив MAC адрес настраиваемого интерфейса. Далее в появившемся поле ввода указать IP адрес и маску сети в формате «x.x.x.x/xx» и нажать кнопку «ок» для сохранения.

Удаление настроек интерфейса из конфигурации узла фильтрации осуществляется путем нажатия на пиктограмму × слева от названия интерфейса.

В строке «Шлюз» указан шлюз по умолчанию (default gateway) для маршрутизации трафика. Для корректировки его параметров необходимо нажать на пиктограмму и указать новый IP адрес.

### 3.4.3 Маршрутизация

Данный модуль предназначен для указания статических маршрутов сетевого трафика, которые будет иметь приоритет перед маршрутом по умолчанию. Интерфейс модуля представлен ниже (Рисунок 25).

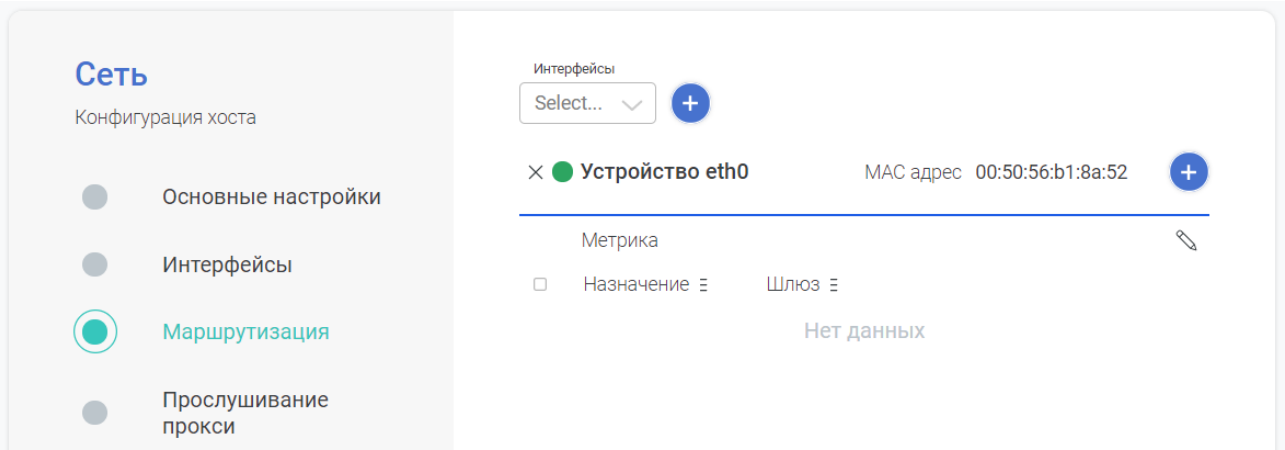


Рисунок 25 – Интерфейс конфигурации статических маршрутов

Для задания статического маршрута нужно:

1. Нажать пиктограмму напротив имени интерфейса. Выбор интерфейса осуществляется в зависимости от указанного шлюза (должны быть в одной подсети);
2. В появившемся поле ввода «Назначение» указать адрес сети или хоста в формате x.x.x.x\xx;
3. В поле ввода «Шлюз» указать IP адрес шлюза, через который должны осуществляться маршрутизация трафика к заданной сети\хосту;
4. Нажать кнопку «Ок»;
5. В случае необходимости, задать метрику маршрута в строке «Метрика».

Удаление статического маршрута осуществляется путем нажатия на пиктограмму × напротив параметров маршрута.

### 3.4.4 Прослушивание прокси

В данном модуле задаются настройки подключения пользователей к узлу фильтрации для получения доступа в интернет (Рисунок 26).

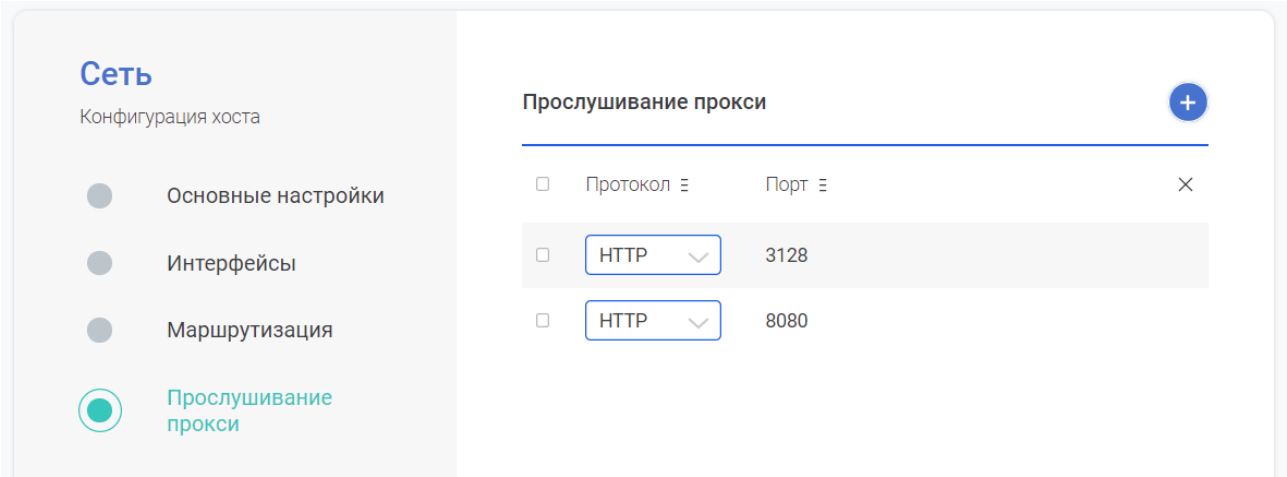


Рисунок 26 – Конфигурация портов подключения к узлу фильтрации

Добавление дополнительных портов для подключения необязательно, по умолчанию в системе преднастроены два порта – 3128 и 8080 с использованием протокола HTTP(S).

Для добавление дополнительного порта необходимо нажать на пиктограмму + и выбрать используемый протокол из выпадающего меню, а также задать порт подключения, после чего нажать кнопку «Ок».

Удаление порта подключения осуществляется путем выставления отметки напротив нужного порта и нажатием на пиктограмму × .

## 3.5 Разбор SSL трафика

Система предусматривает механизм разбора HTTPS сессий пользователей с целью инспектирования контента, передаваемого в рамках этих сессий. Интерфейс настройки данного механизма расположен в разделе «Базовые настройки» в меню «SSL» (Рисунок 27).

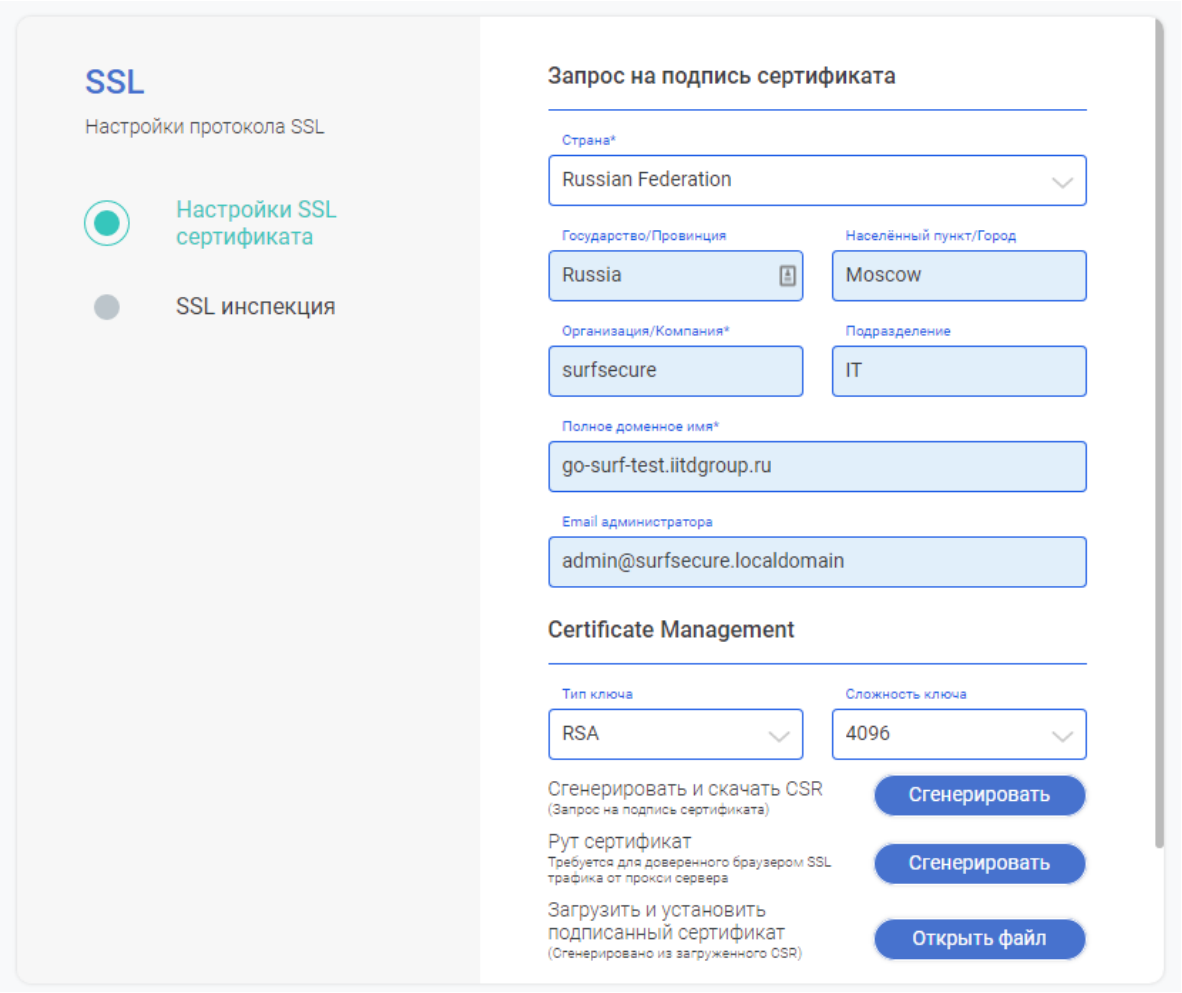


Рисунок 27 – Интерфейс настройки параметров разбора SSL

Для корректной работоспособности данного механизма необходимо сформировать цифровой сертификат, на базе которого будет происходить разбор трафика. Для этого необходимо заполнить следующие поля в области «запрос на подпись сертификата»:

- Страна;
- Государство;
- Населенный пункт\Город;
- Организация\Компания;
- Подразделение;
- Полное доменное имя;
- Email администратора.

Поле «Полное доменное имя» должно полностью совпадать с доменным именем узла фильтрации, которое было назначено при установке системы.

Существует два основных сценария формирования сертификата:

- Использование самоподписанного сертификата;
- Использование сертификата, подписанного корпоративным центром сертификации.

Если в корпоративной инфраструктуре существует центр сертификации, с которым настроено доверие для всех АРМ пользователей, то на узле фильтрации необходимо сформировать запрос на подпись сертификата. Для этого необходимо нажать кнопку «Сгенерировать» напротив поля «Сгенерировать и скачать CSR», после чего будет выполнена загрузка файла-запроса на рабочую станцию администратора. Далее скачанный файл-запрос необходимо передать администратору корпоративного центра сертификата с целью подписи и выпуска файла-сертификата. Выпущенный файл-сертификат необходимо импортировать в узел фильтрации, для этого в меню «SSL» необходимо нажать кнопку «Открыть файл» и указать путь к файлу сертификату. По окончанию импорта будет отображено всплывающее окно с информацией о корректности установки сертификата. Рекомендации по выпуску сертификата на корпоративном центре сертификации приведены в приложении 1.

В случае отсутствия корпоративного центра сертификации необходимо использование самоподписанного сертификата – для этого необходимо нажать кнопку «Сгенерировать» напротив поля «Рут сертификат», в результате чего внутри узла фильтрации сформируется сертификат и дополнительно начнется его загрузка на рабочую станцию. Следующим шагом необходимо обеспечить доверие данному сертификату для всех АРМ пользователей системы, например, с использованием инструмента групповых политик и добавлением данного сертификата в доверенные корневые сертификаты. Также возможно выполнить локальную настройку АРМ и внести сертификат в доверенные, для этого необходимо открыть веб-обозреватель Internet Explorer, войти в меню настройки и выбрать пункт «Свойства браузера». Далее перейти на вкладку «Содержание», нажать кнопку «Сертификаты», в результате чего отобразится интерфейс работы с сертификатами АРМ, и в нем открыть вкладку «Доверенные корневые центры сертификации» (Рисунок 28).

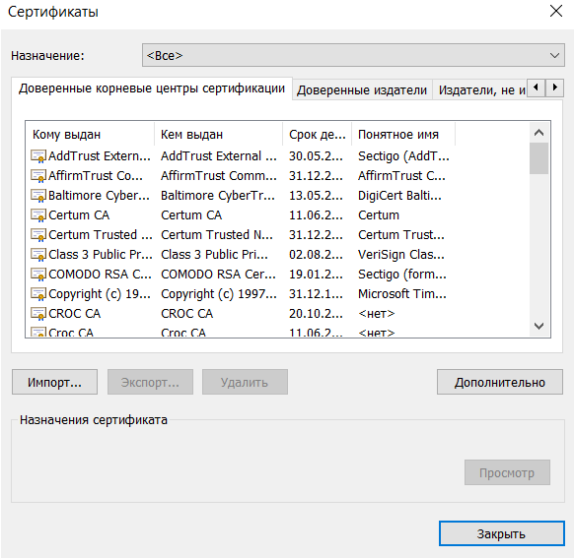


Рисунок 28 – Интерфейс работы с сертификатами

Для добавления сертификата необходимо нажать кнопку «Импорт» и выполнить загрузку самоподписанного сертификата, который был ранее загружен с узла фильтрации.

В случае настройки функционала разбора SSL трафика на системе, где настрое кластер конфигурации – то вышеуказанные действия выполняются только на основном узле. В противном случае – вышеуказанные действия должны быть выполнены на каждом узле

фильтрации в отдельности. По окончанию процедуры настройки сертификатов необходимо нажать кнопку «Сохранить».

Дальнейшая настройка механизма разбора SSL происходит в подразделе «SSL инспекция» (Рисунок 29).

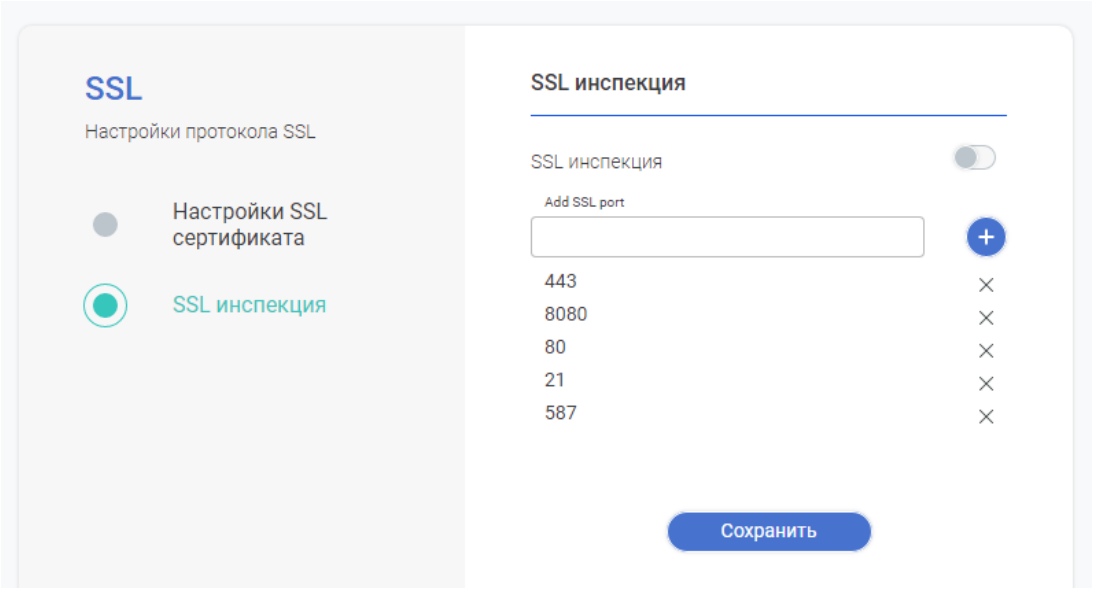


Рисунок 29 – Интерфейс настройки портов для разбора SSL

Чтобы активировать механизма разбора SSL трафика, необходимо нажать на пиктограмму напротив поля «SSL инспекция». Активацию функционала необходимо производить только после корректной настройки параметров SSL сертификата.

В данном меню также представлен перечень портов, по которым пользователи смогут обращаться ко внешним веб ресурсам с использованием протокола HTTPS (для большинства ресурсов это порт 443). В случае, когда необходимо обеспечить доступ по нестандартным портам (например, для обеспечения работы банк-клиентов), их необходимо добавить в настройки системы путем указания порта или нескольких портов через запятую в поле «Add SSL port» и нажатием пиктограммы . После чего данные порты будут отображены в интерфейсе системы. По окончанию настроек необходимо нажать кнопку «Сохранить».

## 3.6 Аутентификация и интеграция с LDAP

Система имеет функционал интеграции с доменным каталогом пользователей Active Directory с целью идентификации пользователей и применения политик разграничения доступа к отдельным пользователям или группе пользователей. Настройка вышеуказанных параметров осуществляется в разделе «Настройки» меню «Аутентификация» (Рисунок 30).

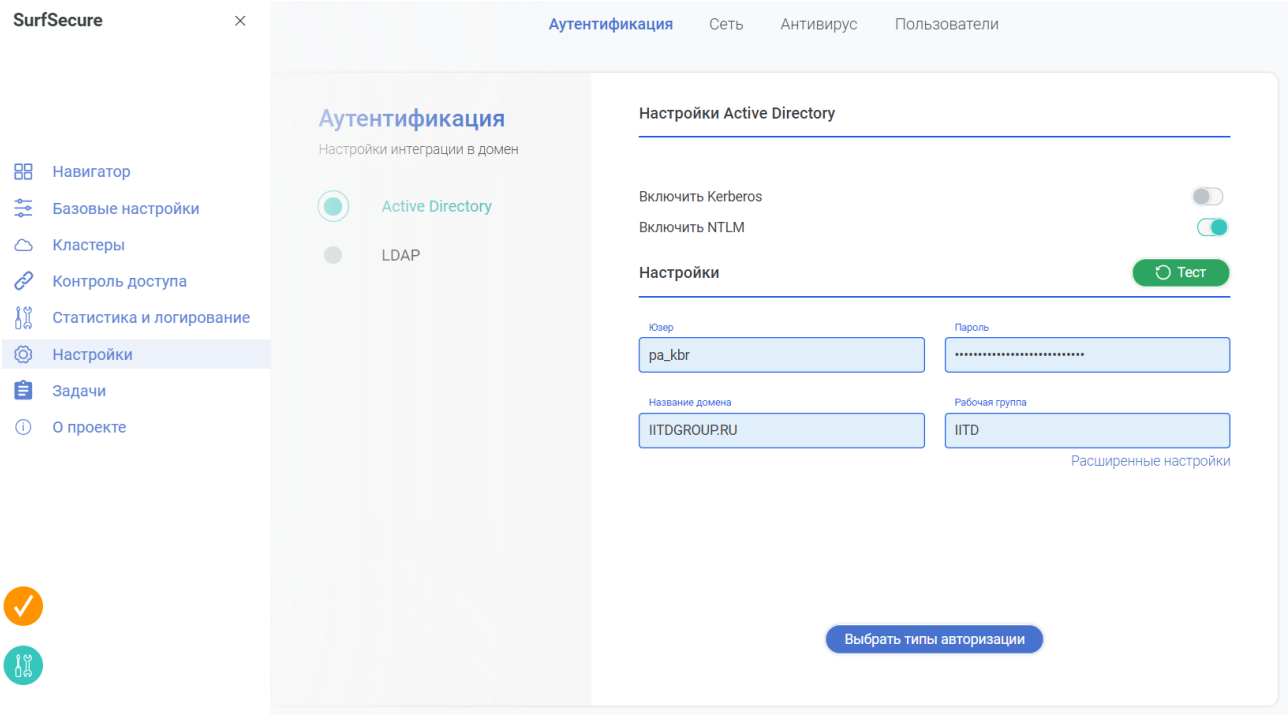


Рисунок 30 – Настройка параметров аутентификации доменных пользователей

В данном меню представлены два основных модуля:

- Active Directory – указываются параметры интеграции с Active Directory для аутентификации пользователей с использованием «прозрачной аутентификации», а также выбор методов аутентификации;
- LDAP – указываются параметры интеграции с LDAP каталогом для Basic-аутентификации пользователей, импорта доменных пользователей и групп в систему, с целью обеспечения возможности их использования при формировании правил доступа.

### 3.6.1 Интеграция с Active Directory

Модуль интеграции с Active Directory (Рисунок 31) представляет собой интерфейс, в котором указываются параметры по подключению к Active Directory, а также выбор протокола для аутентификации пользователей.

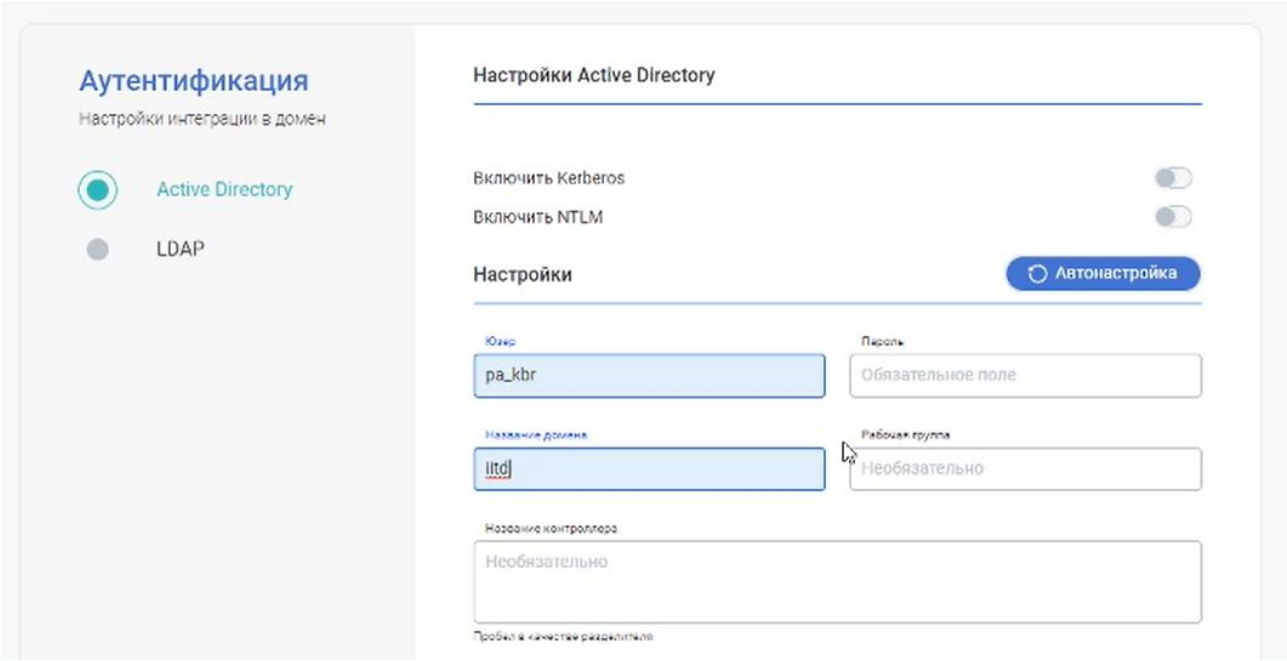


Рисунок 31 – Модуль настройки подключения к Active Directory

Первично необходимо настроить подключение узла фильтрации к каталогу Active Directory, для этого необходимо указать следующие параметры:

- Юзер – учетная запись для подключения;
- Пароль – пароль от указанной учетной записи;
- Название домена – FQDN имя домена (например – domain.local).

После ввода данных параметров необходимо нажать кнопку «Автонастройка», что приведет к автоматическому заполнению оставшихся полей «Рабочая группа» (Netbios имя домена) и «Название контроллера» (FQDN имена контроллеров домена), если это возможно. Поле «Название контроллера» скрыто по умолчанию и для его отображения требуется нажать ссылку «Расширенные настройки». В случае возникновение ошибки автозаполнения, данные поля необходимо указать вручную. Для поля «Название контроллера» допустимо указание нескольких контроллеров домена через пробел, либо указания символа «*» для обеспечения автоматического получения перечня контроллеров домена и реализации отказоустойчивости между ними. По окончанию ввода данных настроек необходимо нажать кнопку «Выбрать тип авторизации» для сохранения указанных параметров.

Следующим шагом необходимо выбрать один или несколько способов аутентификации пользователей:

- Включить Kerberos – для использования протокола Kerberos;
- Включить NTLM – для использования протокола NTLM.

Если выбраны оба протокола аутентификации, то будет использован сначала протокол Kerberos, а в случае возникновения ошибки – протокол NTLM.

Для сохранения настроек выбора протоколов аутентификации необходимо нажать кнопку «Выбрать тип авторизации», применить изменения и протестировать корректность работы механизмов кнопкой «Тест». Результат тестирования будет отображен в текстовом виде в нижней области интерфейса настройки параметров подключения.

Для использования протокола аутентификации Kerberos необходимо соблюдение требований, указанных в таблице 1.

Таблица 1 – Требования для интеграции по протоколу Kerberos

| | |
|---|---|
| Сетевое взаимодействие | • Доступ к контроллерам домена по портам:<br>  ○ TCP/445<br>  ○ TCP/139<br>  ○ TCP/88<br>  ○ UDP/88<br>• Доступ к доменным DNS серверам по порту UDP/53;<br>• Доступ к доменному NTP серверу по порту UPD/123. |
| Настройки DNS | • Для всех узлов фильтрации должны быть созданы А-записи на доменных DNS серверах.;<br>• Должно быть обеспечено корректное разрешение доменных имен узлов фильтрации и контроллеров домена на самих узлах фильтрации и на АРМ пользователей;<br>• В случае использования кластера – необходимо обеспечить выполнение вышеуказанных условий и для кластерного IP адреса. |
| Время | • На всех узлах фильтрации, а также контроллерах домена должно быть синхронизировано время и выставлены корректные часовые пояса. |
| Учетная запись для подключения | • Должен быть создан сервисные аккаунт для подключения к Active Directory;<br>• Для созданного аккаунта должны быть активированы следующие свойства:<br>  ○ User cannot change password;<br>  ○ Password never expires;<br>  ○ This account support Kerberos aes 128/256 (опционально для поддержки AES);<br>  ○ Все остальные свойства должны быть деактивированы.<br>• Данный аккаунт должен иметь права на ввод компьютера в домен;<br>• Для учетной записи необходимо создать следующие SPN записи:<br>  ○ FQDN имен всех узлов фильтрации;<br>  ○ FQDN имени кластера\виртуального IP.<br><br>Создание SPN записи возможно командой «setspn -U -S HTTP/proxy1.domain.com service_account_username». |

| | |
|---|---|
| Настройки браузера пользователей | • Обращение пользователей к узлам фильтрации или кластерному адресу должно осуществляться по FQDN имени. |

### 3.6.2 Интеграция с LDAP

Настройки интеграции с LDAP позволят осуществить импорт доменных пользователей и групп внутрь узла фильтрации с целью их последующего использования в процессе формирования индивидуальных или групповых политик доступа в интернет. Кроме того, данная настройка необходима для реализации Basic аутентификации пользователей, которая будет использована в случае, если аутентификация через Kerberos или NTLM невозможна. Также данный шаг необходим для обеспечения авторизации администраторов системы под доменной учетной записью (назначение прав доступа описано в п. 3.9) в веб интерфейсе управления узла фильтрации. Перечень существующих коннекторов с LDAP каталогом отображен в основном интерфейсе модуля (Рисунок 32).

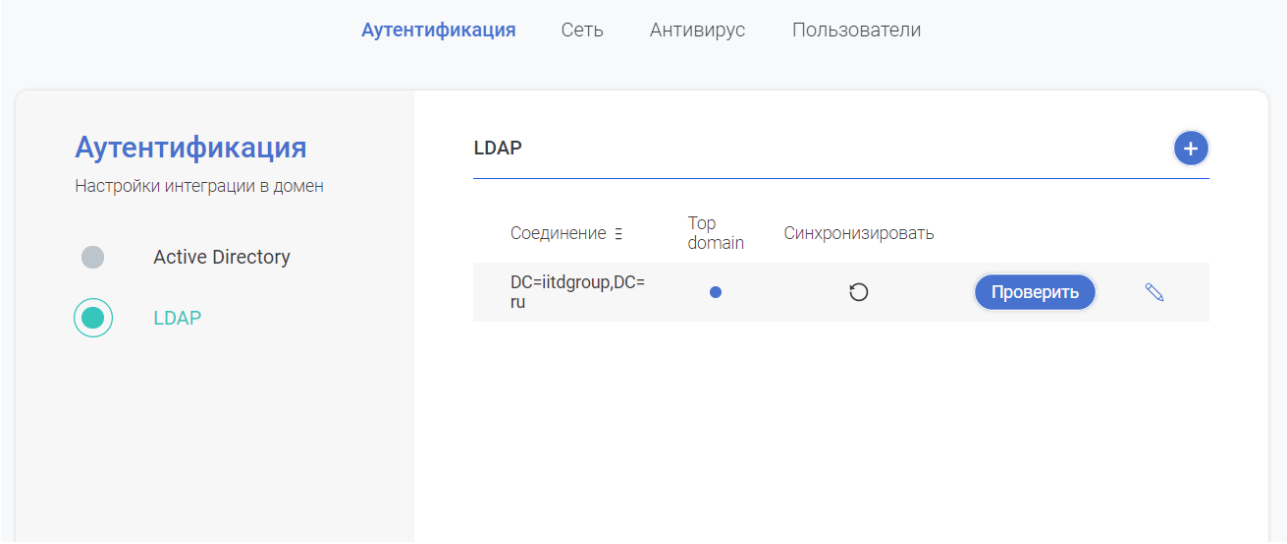


Рисунок 32 – Параметры интеграции с LDAP

Интерфейс содержит в себе следующие возможности по настройки и управлению:

- Кнопка «Проверить» - инициирует процесс подключения к выбранному LDAP коннектору, результат проверки отображается во всплывающем окне;
- - инициирует принудительный процесс синхронизации пользователей и групп пользователей через выбранный коннектор. В случае успешной синхронизации, необходимо нажать кнопку «Apply settings» для применения изменений в перечне импортированных пользователей и групп;
- - редактирование параметров существующего LDAP коннектора.
- Маркер «Top domain» - обозначает домен по умолчанию (может быть выбран только один домен). Данная настройка указывает на LDAP коннектор, к которому будет осуществлен запрос по аутентификации пользователя, если он

не указал префикс домена (например, domain\user или user@domain.local) в своём логине. Может принимать следующие значения:

  - Синий – данный коннектор выбран как домен по умолчанию;
  - Серый – данный коннектор не является доменом по умолчанию.

- - добавить новый LDAP коннектор.

Чтобы добавить новый LDAP коннектор необходимо нажать кнопку , после чего отобразится интерфейс ввода параметров (Рисунок 33).

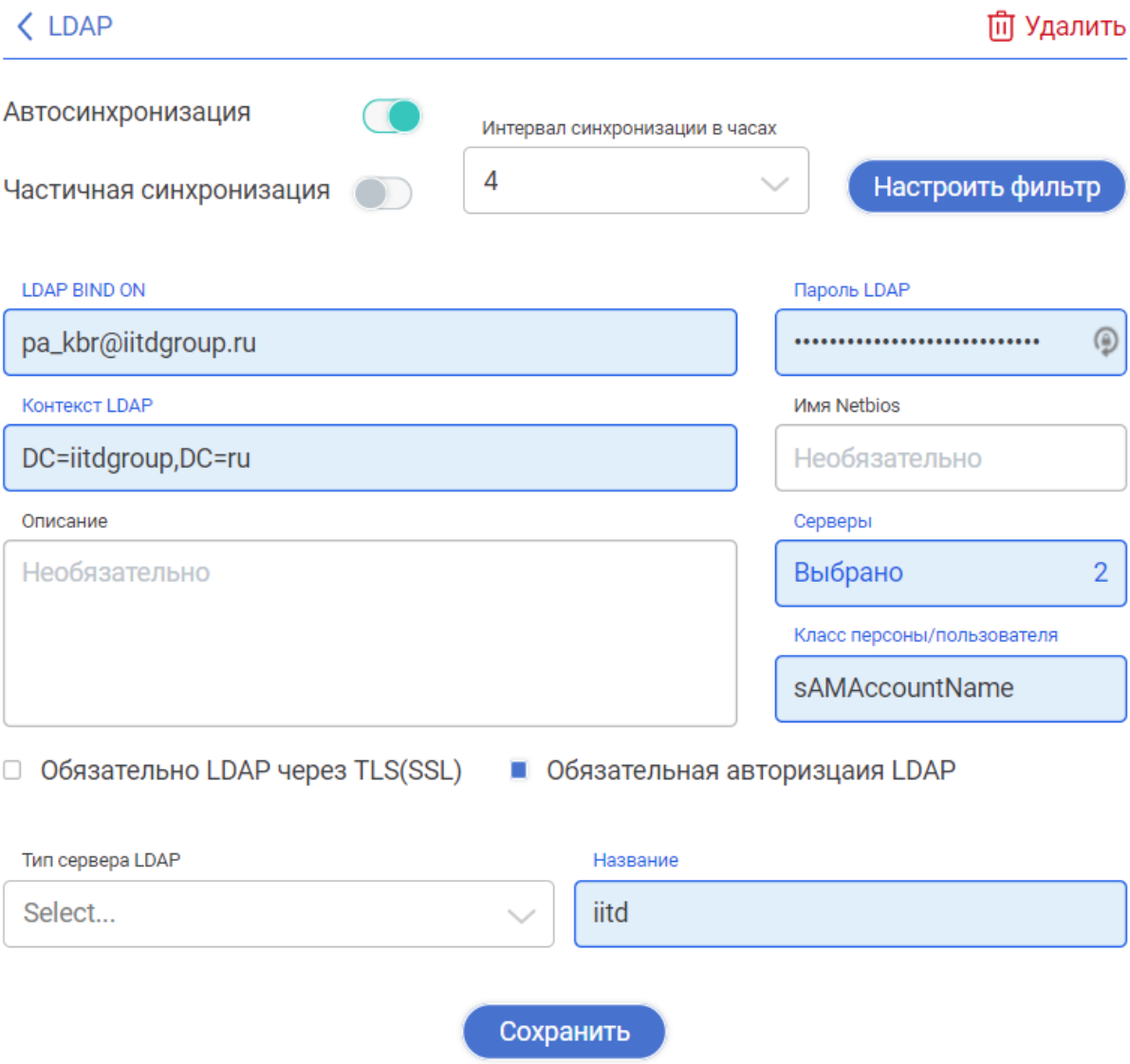


Рисунок 33 – Параметры LDAP коннектора

Для настройки LDAP коннектора необходимо указать следующую информацию:

- Указать обязательные параметры подключения:
  - LDAP BIND DN – учетная запись для подключения к LDAP в формате «user@domain.local»;
  - Пароль LDAP – пароль от указанной учетной записи;
  - Контекст LDAP – каноническое имя LDAP;

    - Серверы – указать перечень домен контроллеров для подключения (возможно использовать кнопку автонастройки для автоматического импорта параметров);
    - Название – имя создаваемого LDAP коннектора;
- Указать необязательные параметры подключения:
    - Netbios имя домена;
    - Класс персоны/пользователя – атрибут пользователя содержащего его логин (если параметр не задан – используется значение sAMAccountName);
    - Описание созданного коннектора.
    - Необходимость подключение к LDAP с использованием TLS шифрования;
    - Необходимость авторизации в LDAP.
- Указать информацию о LDAP сервере:
    - Тип сервера LDAP – указать тип системы (Windows или openLDAP)
- Указать настройки по синхронизации коннектора:
    - Автосинхронизация – при включении данной опции через заданный промежуток времени будет инициирован процесс синхронизации узла фильтрации с LDAP сервером;
    - Частичная синхронизация – при включении данной опции в рамках процесса синхронизации будут загружены только изменения по созданным\удаленным пользователям или группам пользователей;
    - Интервал синхронизации в часах – временной промежуток в часах между процессами автосинхронизации.

Далее необходимо нажать кнопку «Настроить фильтр», в результате чего отобразиться окно для указания фильтров LDAP запросов (Рисунок 34).

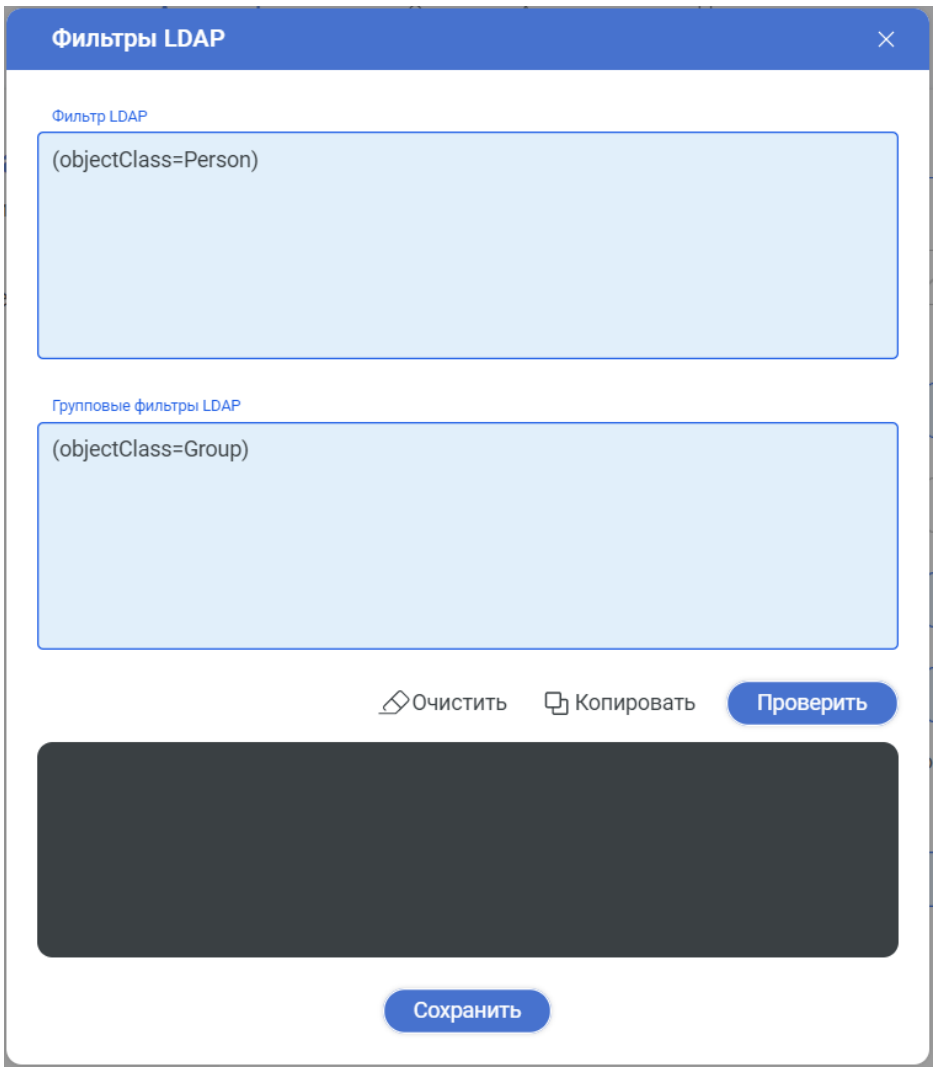


Рисунок 34 – Настройка фильтров LDAP запросов

В данном интерфейсе указываются фильтры пользователей и групп, которые будут импортированы из LDAP каталога в результате синхронизации коннектора. Фильтры указывается с использованием LDAP синтаксиса, на вышеуказанном рисунке указаны стандартные параметры для интеграции с доменом Active Directory. Все объекты, не попадающие под заданные фильтры, в систему импортироваться не будут.

Для сохранения настроек коннектора необходимо нажать кнопку «Сохранить», после чего произойдет переадресация на основную страницу с перечнем коннекторов. Обязательным шагом является проверка корректности настройки коннектора, для этого напротив созданного коннектора необходимо нажать кнопку «Проверить», в результате чего будет отображено количество пользователей и групп, которые соответствуют данным критериям запроса.

Для удаления LDAP коннектора необходимо зайти в интерфейс редактирования его параметров путем нажатия пиктограммы  и в верхней правой части нажать кнопку «Удалить».

В случае удаление LDAP коннектора, то из системы будут удалены все пользователи, группы пользователей, которые связаны с этим коннектором. Также будут удалены все политики доступа, связанные с данными пользователями и группами.

## 3.7 Интеграция с DLP сервером

Система предусматривает возможность интеграции с внешним DLP сервером по протоколу ICAP с целью дополнительной проверки обрабатываемого трафика пользователей на предмет соответствия принятым политикам работы с конфиденциальной информации. Настройка данного взаимодействия осуществляется в разделе «Базовые настройки» в меню «Настройка ICAP» (Рисунок 35).

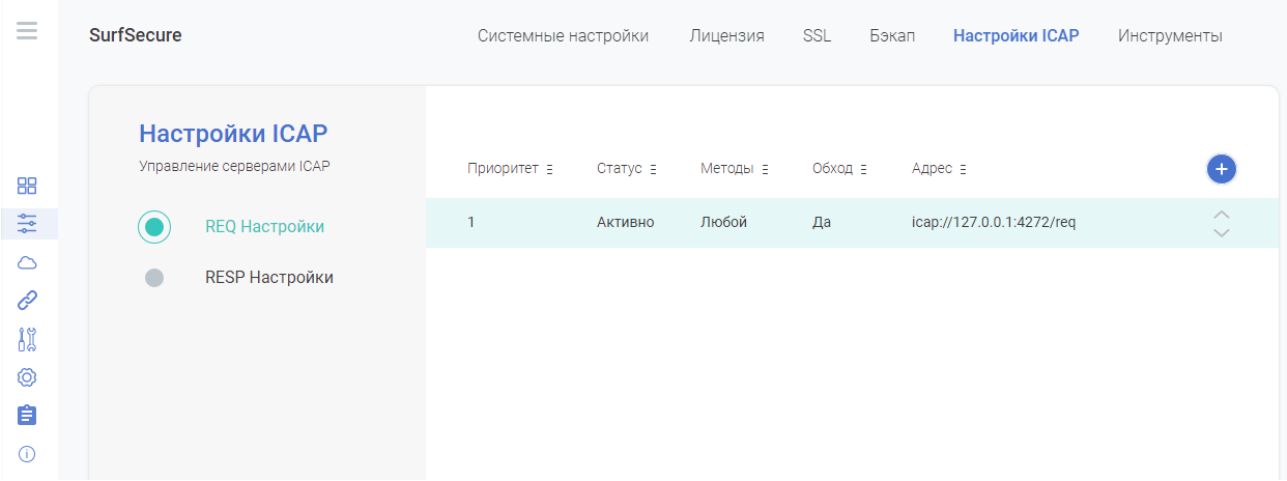


Рисунок 35 – Интерфейс настройки интеграции с DLP системой

Настройка интеграции с внешней DLP системой осуществляется в модуле «REQ Настройки». В системе предустановлен ICAP сервер по умолчанию 127.0.0.1 (отображен в модулях REQ и RESP), данный сервер необходим для корректной работы правил фильтрации. Без явной необходимости или соответствующего указания специалиста технической поддержки отключение сервера ICAP по умолчанию недопустимо.

Для добавления параметров интеграции с внешним ICAP серверов необходимо нажать на пиктограмму  , после чего отобразиться окно конфигурации (Рисунок 36).

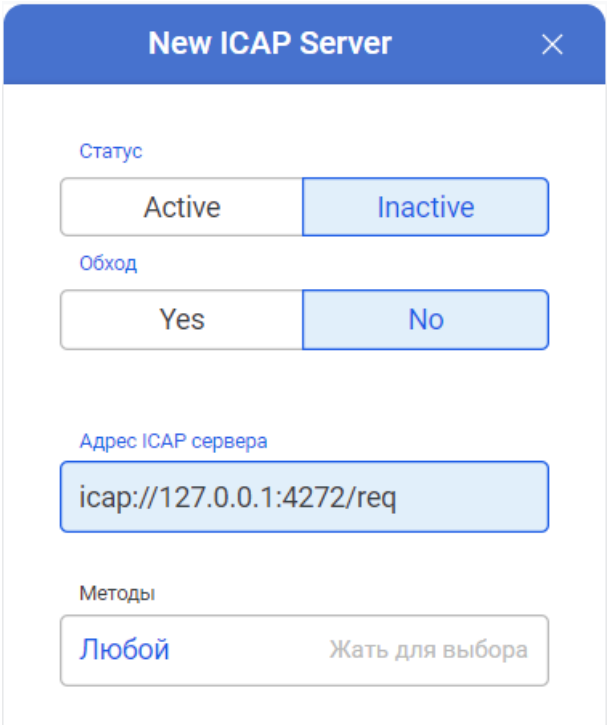


Рисунок 36 – Окно конфигурации внешнего DLP сервера

В данном окне необходимо указать следующие параметры:

- Статус:
  - Active – активный;
  - Inactive – неактивный;
- Обход:
  - Yes – в случае недоступности DLP сервера запрос не будет заблокирован;
  - No – в случае недоступности DLP сервера запрос будет заблокирован;
- Адрес ICAP сервера – IP адрес или FQDN имя с запросом (детальную информацию можно получить у администратора DLP системы);
- Методы – необходимо выбрать необходимые методы взаимодействия или создать собственные (детальную информацию можно получить у производителя DLP системы).

По окончанию ввода параметров интеграции необходимо нажать кнопку «Сохранить».

Настройки системы поддерживают указание приоритетов обработки запросов внешними DLP системами. Для корректировки приоритета конкретного DLP сервера необходимо использовать пиктограмму ⌃⌄ в правой части меню.

Редактирование параметров созданного DLP сервера осуществляется путем нажатия на область строки соответствующей редактируемому узлу, после чего в правой части экрана отобразится всплывающее окно с параметрами интеграции. В случае изменения параметров необходимо нажать кнопку «Сохранить» для внесения изменений.

## 3.8 Защита от вредоносного ПО

Настройки механизма защиты от вредоносного по располагаются в разделе «Настройки» в меню «Антивирус» (Рисунок 37).

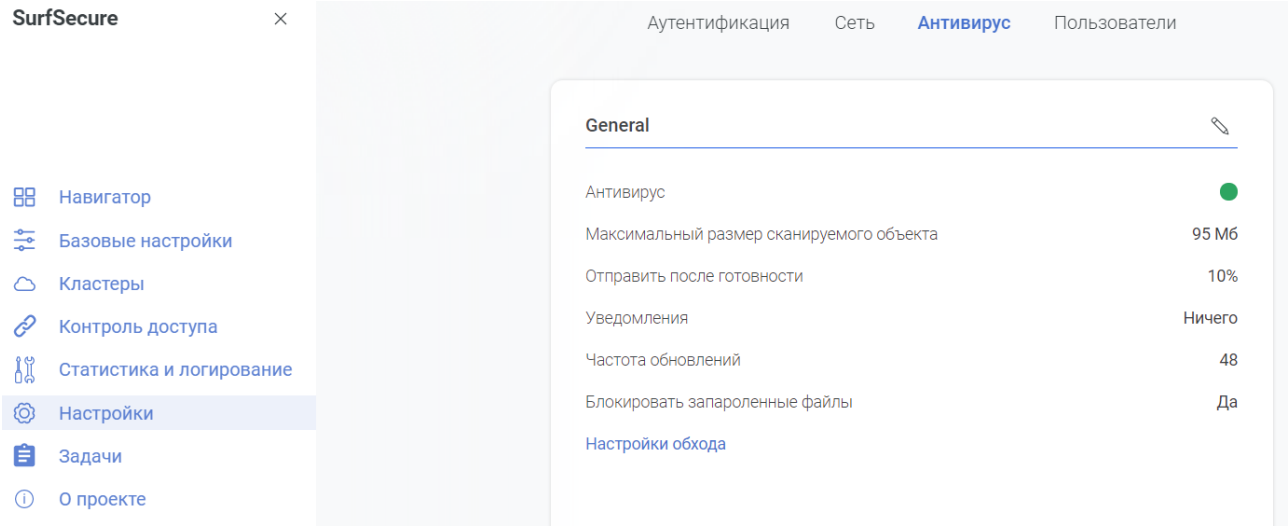


Рисунок 37 – Параметры механизма защиты от вредоносного ПО

Интерфейс позволяет просматривать и корректировать следующие параметры работы механизма путем нажатия на пиктограмму :

- Антивирус – отображает статус работы сервиса:
  - Зеленый – корректная работа;
  - Серый – ошибка или отключен.
- Максимальный размер сканируемого объекта – максимальный размер загружаемого файла, который будет проверен механизмом выявления вредоносного ПО. В случае превышения размера файла заданной настройки – будет проверен тот объем файла от начала загрузки, который задан в данном параметре;
- Отправить после готовности – указание порогового значения объема проверенного файла в % от его общего объема, после которого начинается процесс передачи данного файла в сторону пользователя;
- Уведомления – выбор уровня системных сообщений, создаваемых механизмом защиты от вредоносного ПО, в случае возникновения которых администраторам системы будет отправлено почтовое уведомление. Возможно указание следующих уровней:
  - Все – будут отправляться все сообщения об успешном\неуспешном обновлении и ошибках работы;
  - Ошибки – будут отправляться уведомления об ошибках обновления и работы механизма;
  - Ничего – оповещения не отправляются.
- Частота обновлений – временной интервал в часах, через который будут запрошены обновления сигнатур механизма;

- Блокировать запароленные файлы – для таких файлов невозможно осуществить проверку механизмом защиты от вредоносного ПО, поэтому можно предусмотреть блокировку их передачи.

Существует возможность настройки исключения проверки файлов данных механизмом, для этого необходимо нажать на ссылку «Настройки обхода», которая отобразит интерфейс по работе с необходимыми параметрами (действия по настройке параметров обхода отражены п. 3.11).

Интерфейс также предусматривает возможность ручного обновления:

- Начать обновления сигнатур – обновление сигнатур вредоносного ПО;
- Update site classifier signatures – обновление сигнатур классификации веб ресурсов.

Для принудительного обновления необходимо нажать кнопку «Обновить» напротив необходимого механизма, а также включить опцию «Полное», если необходимо полное обновление баз данных с удалением имеющейся информации по сигнатурам.

## 3.9 Пользователи и роли

Работа с пользователями системы, а также назначение полномочий доступа к системе осуществляется в разделе «Настройки» в меню «Пользователи» (Рисунок 38).

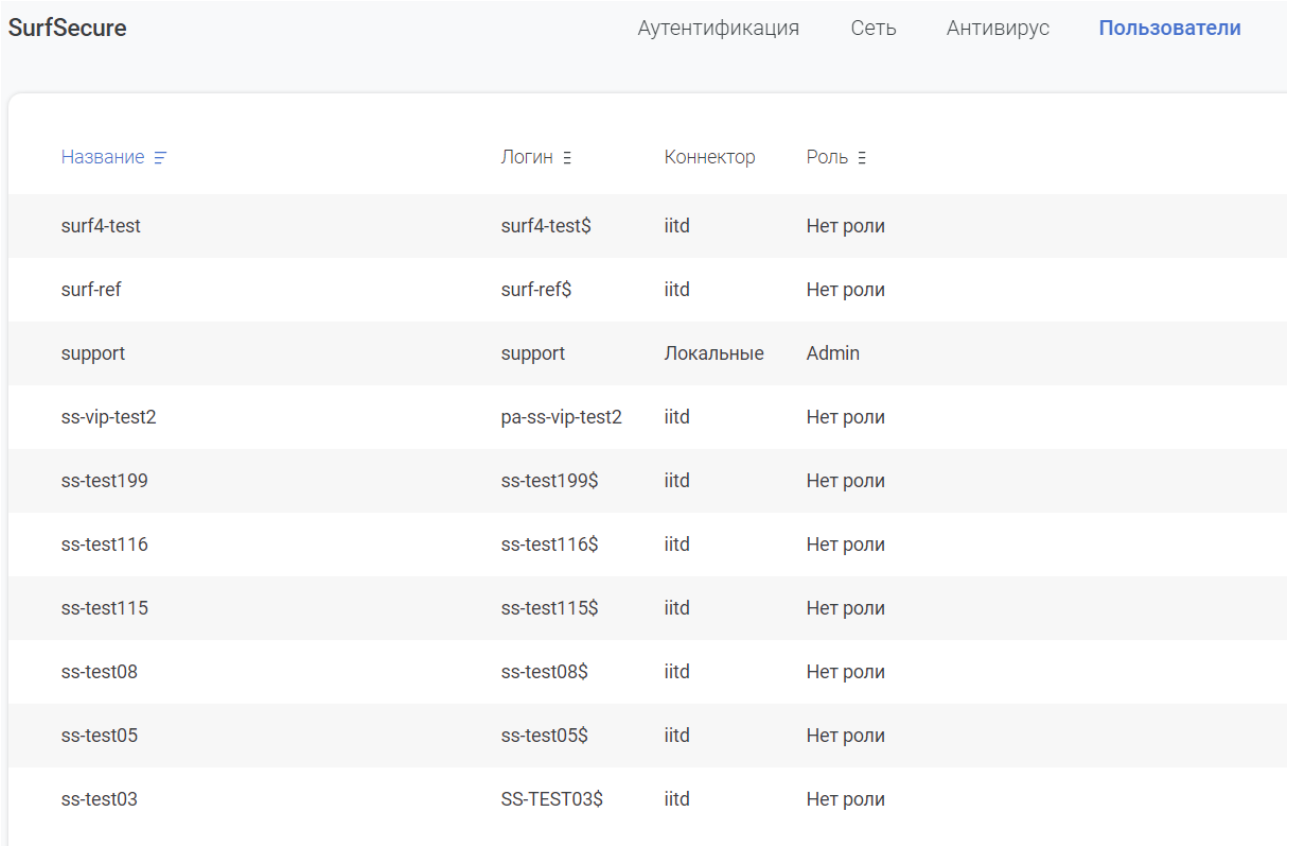


Рисунок 38 – Интерфейс просмотра пользователей системы

В данном интерфейс будет отображен весь перечень пользователей системы, который состоит из локальных учетных записей внутри узла фильтрации и импортированных

пользователей через коннектор к LDAP каталогу. Для каждого пользователя отображены следующие параметры:

- Название – имя пользователя;
- Логин – имя учетной записи пользователя;
- Коннектор – наименование коннектора LDAP, через который был импортирован пользователь;
- Роль – назначенная роль в системе для данного пользователя.

Некоторые пользователи могут быть выделены серым цветом – это означает, что учетная запись в LDAP каталоге находится в статусе «Отключено\Disabled». Для работы со списком пользователей возможно использование следующих инструментов:

- - поиск пользователя по его логину;
- - сортировка по выбранному параметру;
- 1/37 - навигация по страницам.

Для редактирования параметров пользователя необходимо нажать на строку с информацией о пользователе, после чего отобразиться дополнительное информационное окно. Редактирование параметров осуществляется путем нажатия пиктограммы в дополнительном окне в указания следующих параметров:

- Для доменных пользователей:
  - Роль – применение одной из ролей для доступа к интерфейсу управления;
- Для локальных учетных записей:
  - Название – имя учетной записи;
  - Логин – учетная запись для входа;
  - Эл. Почта – почтовый адрес для оповещений;
  - Роль – полномочия пользователя в системе;
  - Пароль\Подтверждение пароля – парольная фраза учетной записи, не менее 6-ти символов;

Создание новой локальной учетной записи осуществляется путем нажатия пиктограммы и ввода параметров, описанных выше. Удаление учетной записи осуществляется путем нажатия пиктограммы напротив информации о пользователе, возможно удаление только вновь созданных локальных учетных записей. По окончанию редактирования или создания учетной записи необходимо нажать кнопку «Сохранить».

Модель ролевого разграничения системы представлена в таблице 2.

Таблица 2 – Ролевая модель

| Роль\права | Контроль доступа | Системные настройки |
|---|---|---|

| | | |
|---|---|---|
| Admin | Просмотр и правка | Просмотр и правка |
| Manager | Просмотр | Просмотр |
| Officer | Чтение и редактирование | - |
| No role | - | - |

Для предустановленной учетной записи «Support» установлена роль Admin и её изменение возможно лишь другой учетной записью с правами Admin, таким образом в системе всегда будет оставаться хотя бы одна привилегированная учетная запись.

## 3.10 Отказоустойчивость и кластеризация

Система позволяет реализовать механизмы централизованного управления и кластеризации, в случае, когда архитектурой предусмотрено использование несколько узлов фильтрации одновременно. Существуют следующие режимы работы:

- Кластер конфигурации;
- Кластер балансировки.

Кластер конфигурации обеспечивает синхронизацию настроек фильтрации для нескольких узлов фильтрации одновременно. Для этого выделяется один основной узел фильтрации, к которому подключаются вспомогательные узлы, и при изменении политик фильтрации пользовательского трафика на основном узле фильтрации – данные изменения будут отправлены на остальные вспомогательные узлы. После окончания настройки кластера конфигурации все настройки необходимо осуществлять на основном узле фильтрации.

Кластер балансировки нагрузки позволяет осуществлять автоматическое распределение пользовательского трафика между несколькими узлами фильтрации, причем распределение трафика возможно корректировать за счет приоритетов или загруженности узла фильтрации. Настройку кластера балансировки можно осуществить только после настройки кластер конфигурации.

Основным требованием для создания кластера узлов фильтрации является размещение хотя бы одного сетевого интерфейса у всех узлов фильтрации в одной и той же бродкаст-сети для обеспечения сетевого взаимодействия.

Настройка параметров работы узла фильтрации в режиме кластера осуществляется в разделе «Кластеры» (Рисунок 39).

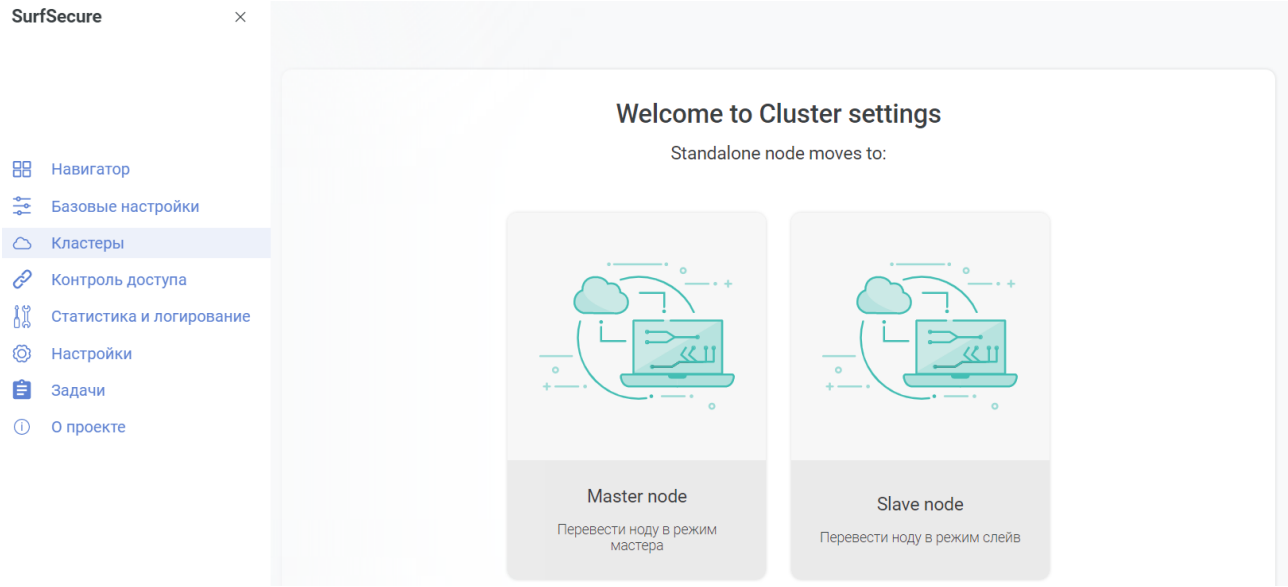


Рисунок 39 – Интерфейс управления режимом кластеризации

### 3.10.1 Настройка кластера конфигурации

Кластер конфигурации состоит из одного основного узла фильтрации (Master node) и одного или нескольких вспомогательных узлов (Slave node). Для создания кластера первоначально необходимо настроить основной узел, а потом осуществлять подключение вспомогательных узлов.

#### 3.10.1.1 Конфигурация основного узла

Для создания основного узла кластера конфигурации необходимо в разделе «Кластеры» выбрать иконку «Перевести ноду в режим мастера» и нажать кнопку «Start setup».

Далее отобразиться окно по выбору сетевого интерфейса, через который будут общаться узлы-участники кластера (Рисунок 40). Основной узел фильтрации в обязательном порядке должен быть доступен через указанный сетевой интерфейс.

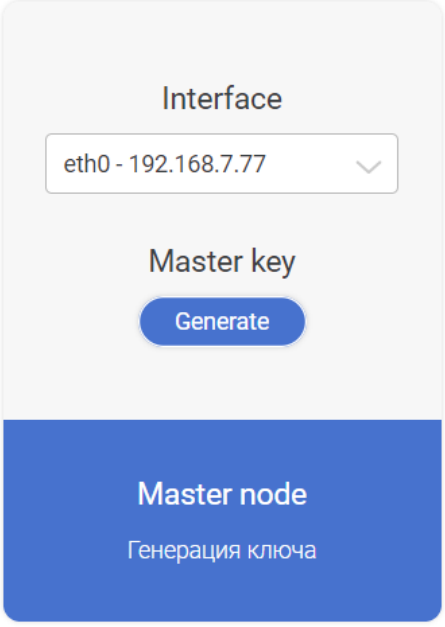


Рисунок 40 – Настройка параметров интерфейса взаимодействия основного узла

На данном шаге необходимо из выпадающего списка выбрать сетевой интерфейс, через который данный узел фильтрации будет взаимодействовать с остальными узлами кластера. После этого необходимо нажать кнопку «Generate» для создание ключа взаимодействия, который впоследствии будет использован для подключения вспомогательных узлов фильтрации к основному. Данный процесс может занимать 5-10 минут, т.к. выполняется процесс перенастройки системы для работы в кластерном режиме. По окончанию процесса будет отображено (Рисунок 41) окно с ключём для подключения вспомогательных узлов фильтрации и приглашением для перехода к интерфейсу настроек кластера.

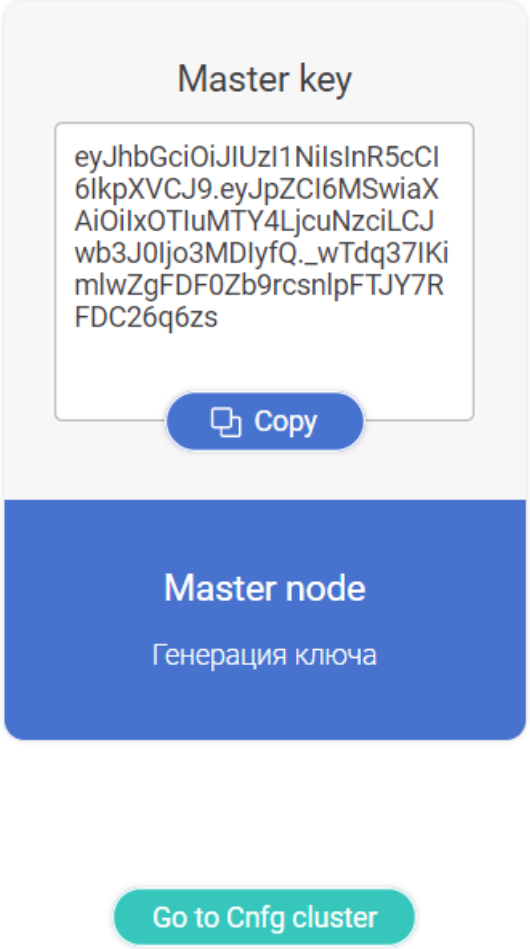


Рисунок 41 – Окно завершения процесса конфигурации основного узла кластера

Указанный ключ необходим в дальнейшем для подключения вспомогательных узлов фильтрации, его можно скопировать в буфер обмена кнопкой «Copy». Для перехода в интерфейс управления кластером (Рисунок 42) нужно нажать на кнопку «Go to Cnfg cluster».

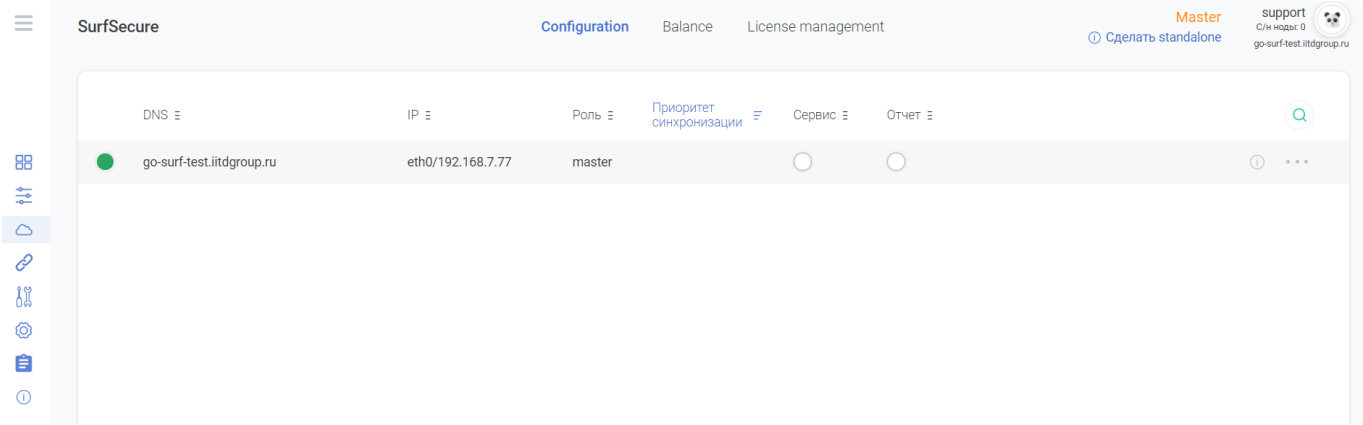


Рисунок 42 – Основной интерфейс конфигурации параметров кластера

Создание кластера конфигурации и управление его настройками описано в разделе 3.10.1.3.

3.10.1.2 Конфигурация вспомогательного узла

Для создания вспомогательного узла кластера конфигурации необходимо в разделе «Кластеры» выбрать иконку «Перевести ноду в режим слейв» и нажать кнопку «Start setup».

Далее отобразиться окно по выбору сетевого интерфейса и указания ключа подключения, через который будет осуществлено подключение к основному узлу кластера (Рисунок 43).

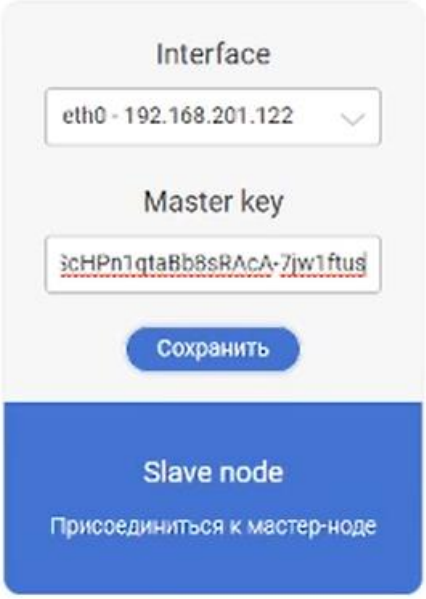


Рисунок 43 – Настройка параметров интерфейса взаимодействия вспомогательного узла

На данном шаге необходимо из выпадающего списка выбрать сетевой интерфейс, через который данный узел фильтрации будет взаимодействовать с остальными узлами кластера. После этого в поле «Master key» необходимо указать ключ подключения к основному узлу кластера (данный ключ генерируется на этапе настройке основного узла и может быть получен в интерфейсе настроек кластера конфигурации) и нажать кнопку «Сохранить». Результатом выполненных действий является начало подключения к основному узлу фильтрации, данный процесс может занимать 5-10 минут, т.к. выполняется процесс

перенастройки системы для работы в кластерном режиме. По окончанию процесса будет отображено окно настроек кластера. По окончанию действий по подключению вспомогательных узлов фильтрации необходимо на основном узле фильтрации перейти в раздел «Кластеры» в меню «Configuration» и убедиться в корректной синхронизации всех узлов – слева от названия отображен индикатор:

- Зеленый – синхронизация успешна;
- Желтый– процесс синхронизации еще не завершен.

После окончания настройки кластера конфигурации все настройки необходимо осуществлять на основном узле фильтрации.

#### 3.10.1.3 Конфигурация параметров кластера конфигурации

Настройка параметров кластера конфигурации осуществляется в разделе «Кластеры» в меню «Configuration» (Рисунок 44).

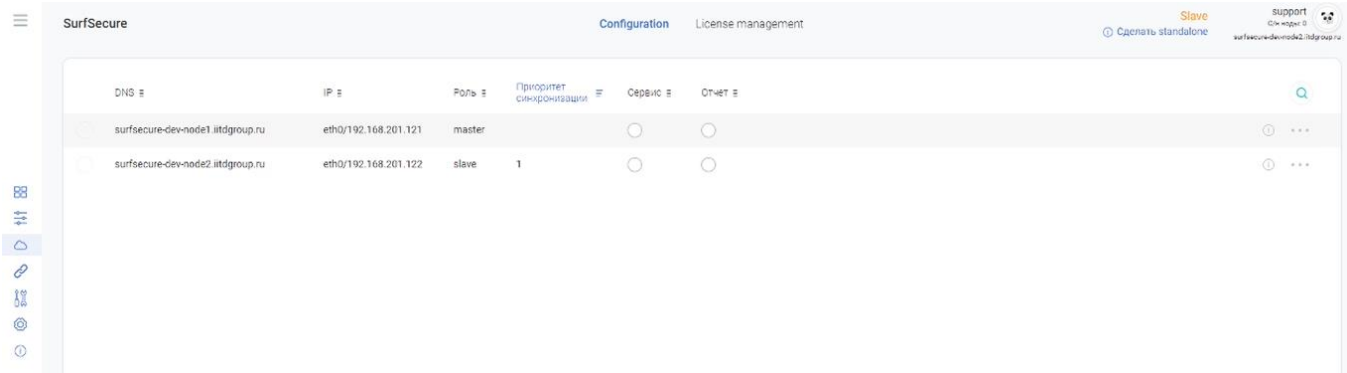


Рисунок 44 – Интерфейс настройки параметров кластера конфигурации

Интерфейс отображает информацию по всем узлам фильтрации, объединенных в кластер, а также позволяет осуществлять редактирование параметров кластера. В правой верхней части интерфейса указан статус узла в кластере, на котором находится администратор:

- Master – основной узел фильтрации;
- Slave – вспомогательный.

Управление настройками кластера должно осуществляться с основного узла кластера, т.к. на вспомогательных узлах доступны не все настройки для редактирования.

Интерфейс отображает следующую информацию по каждому узлу, включенных в кластер:

- Статус – отображается цветной пиктограммой возле имени узла, показывает текущий статус работы узла фильтрации:
  - Зеленый – синхронизация прошла успешно;
  - Оранжевый – синхронизация еще не завершена;
  - Красный – ошибка синхронизации (ошибка отображается в лог системе);
- DNS – имя узла фильтрации;
- IP – отображается сетевой интерфейс, через который осуществляется взаимодействие данного узла с остальными;

- Роль – текущая роль узла в кластере (Master – основной узел, Slave – вспомогательный);
- Приоритет синхронизации – служит для определения порядка применения изменений на нодах после того как они появились на основном узле;
- Сервис – отображается статус настройки механизма обработки трафика:
  -  - сервисы по обработке трафика пользователей включены, узел фильтрации обрабатывает трафик пользователей;
  -  - сервисы по обработке трафика пользователей отключены, узел не обрабатывает трафика пользователей.
- Отчет – отображается статус настройки системы логирования:
  -  - сервисы логирования включены, узел фильтрации локально сохраняет информацию о результатах обработки трафика пользователей, а также формирует статистические отчеты по работе;
  -  - сервисы логирования отключены, узел не сохраняет информацию об обработке трафика пользователей.

Настройка узлов кластера осуществляется путем нажатия на строку с информацией об узле, либо выбора команды «Изменить» из дополнительного меню, доступного через нажатие на пиктограмму . Результатом данных действий будет появление нового окна для конфигурации параметров узла (Рисунок 45).

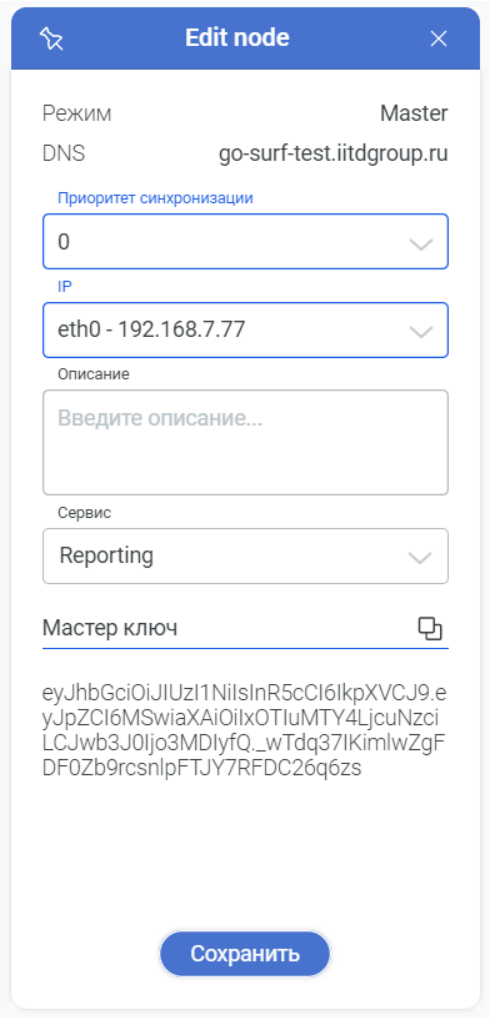


Рисунок 45 – Редактирование параметров узла кластера

В данном интерфейсе необходимо указать следующие параметры:

- Приоритет синхронизации;
- IP – сетевой интерфейс для взаимодействия с остальными участниками кластера (его изменение возможно только в аналогичном разделе меню веб интерфейса администратора узла, для которого требуется изменение);
- Описание – произвольное описание узла фильтрации;
- Сервис – параметры работы механизмов фильтрации и логирования. Параметр может принимать следующие значения:
    - Out of Service – механизмы логирования и фильтрации отключены;
    - Traffic service – включен только механизм фильтрации, узел будет обрабатывать трафик пользователей;
    - Reporting – включен только механизм логирования, узел будет агрегировать логи со всех узлов фильтрации кластера;
    - Traffic service and Reporting – включены оба механизма, узел будет обрабатывать трафик пользователей и сохранять информацию об обработке трафика локально.

- Мастер ключ (отображается только для основного узла) – ключевая последовательность, необходимая для добавления нового вспомогательного узла в кластер конфигурации.

В кластере конфигурации возможно изменение основного узла, для этого в интерфейсе настройки кластера конфигурации основного узла напротив необходимого вспомогательного узла раскрыть дополнительное меню и выбрать команду «Сделать мастером» (Рисунок 46), после чего запустится автоматический процесс перенастройки узлов.

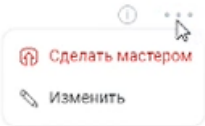


Рисунок 46 – Команда для смены изменения роли узла кластера конфигурации

Удаление узла фильтрации из кластера конфигурации происходит при помощи раздела «Кластера» в локальном веб интерфейсе администратора того узла, который требуется исключить, или на основном узле. Для изменения конфигурации узла необходимо нажать кнопку «Сделать standalone», после чего запустится процесс перенастройки узла фильтрации. Данный процесс может занимать около 5-10 минут. Далее на основном узле кластера конфигурации необходимо перейти в раздел «Кластера» в меню «Configuration» и исключить выбранный узел из состава кластера конфигурации. Для этого необходимо в выпадающем контекстном меню для исключаемого узла выбрать пункт «Удалить» (Рисунок 47).

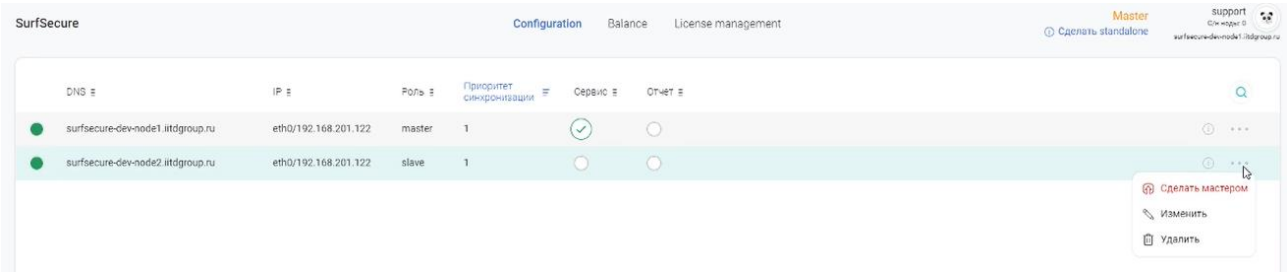


Рисунок 47 – Исключение узла фильтрации из состава кластера конфигурации

### 3.10.2 Настройка кластера балансировки

Настройка кластера балансировки (распределения пользовательского трафика между несколькими узлами фильтрации) осуществляется только после настройки кластера конфигурации. Интерфейс работы с параметрами кластера балансировки доступен на основном узле кластера конфигурации в разделе «Кластера» в меню «Balance» (Рисунок 48).

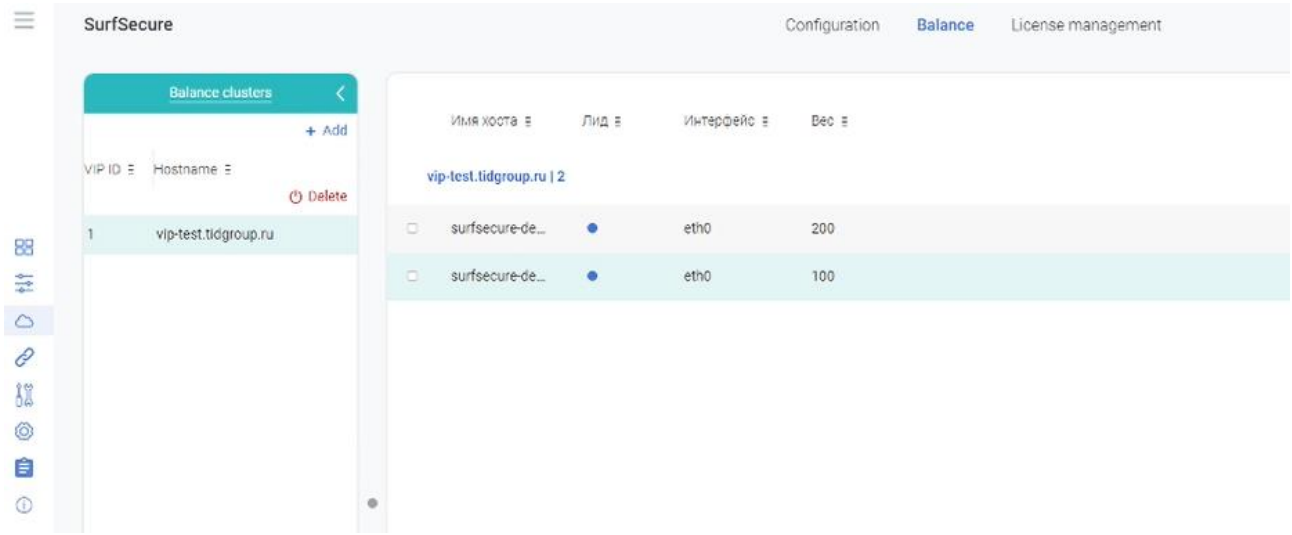


Рисунок 48 – Интерфейс конфигурации кластера балансировки

Для создания кластера балансировки необходимо в области «Balance clusters» нажать кнопку «Add», в результате чего отобразится дополнительное окно с основными параметрами кластера (Рисунок 49).

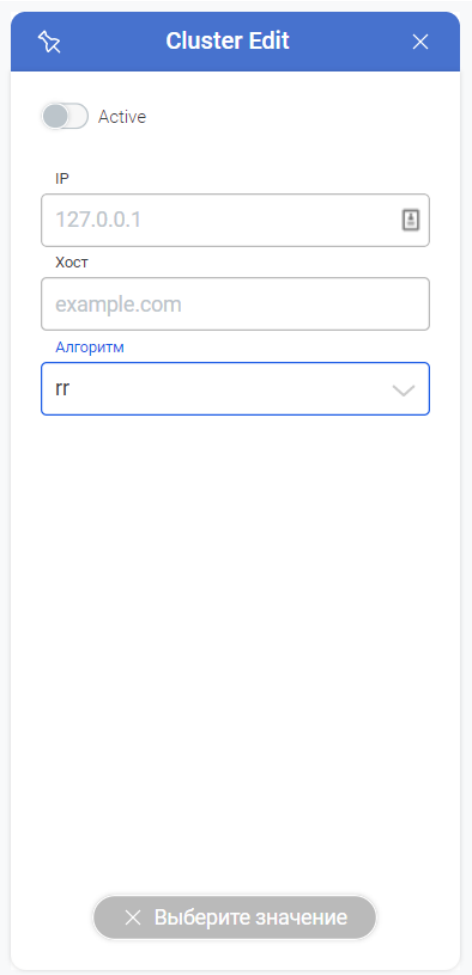


Рисунок 49 – Настройка параметров кластера балансировки

На данном этапе необходимо указать:

- IP - Виртуальный IP адрес кластера, который в дальнейшем будет использоваться как единая точка для подключения пользователей;
- Хост – DNS имя, соответствующее данному IP адресу;
- Алгоритм балансировки нагрузки:
    - rr – распределение трафика между всеми узлами фильтрации, включенных в кластер балансировки;
    - wrr - распределение трафика между всеми узлами фильтрации, включенных в кластер балансировки, с учетом установленного приоритета;
    - lc – распределение трафика между всеми узлами фильтрации, включенных в кластер балансировки, в соответствии с количеством пользовательских подключений;
    - wlc – распределение трафика между всеми узлами фильтрации, включенных в кластер балансировки, в соответствии с количеством пользовательских подключений и учетом установленного приоритета;
- Включить тумблер в поле «Active» для активации кластера балансировки.

После ввода указанных настроек в обязательном порядке необходимо нажать кнопку «Сохранить». По окончанию данных действий в левой части интерфейса отобразиться созданный кластер.

Далее необходимо добавить узлы фильтрации в кластер балансировки, для этого нужно в центральной области интерфейса нажать на пиктограмму , после чего выбрать необходимый узел фильтрации (Рисунок 50) путем отметки пиктограммы напротив имени узла или нескольких узлов, а также указать сетевой интерфейс, который будет участвовать в балансировке трафика (должен быть в одной подсети с виртуальным IP адресом кластера балансировки). Следующим шагом необходимо нажать кнопку «Отправить» для добавления узлов.

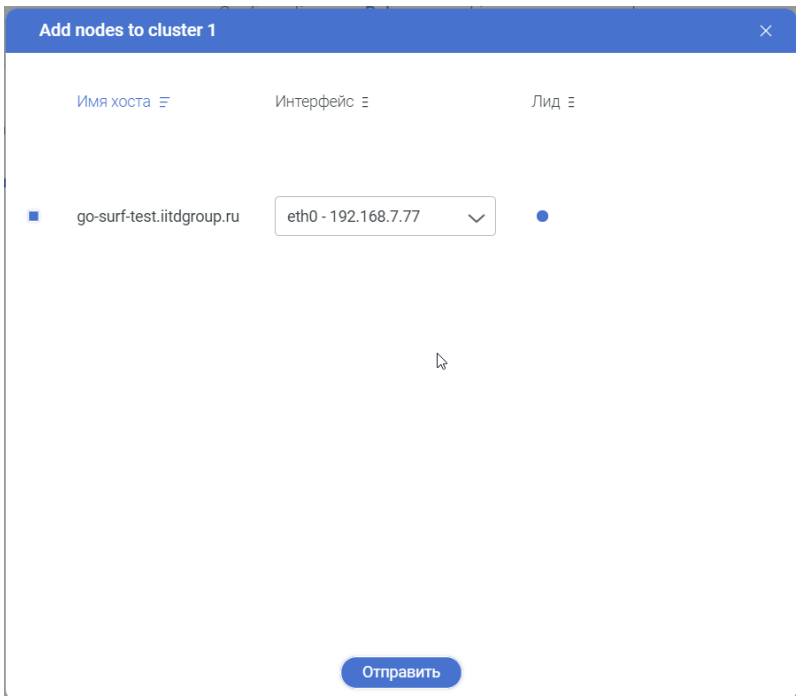


Рисунок 50 – Окно добавления нового узла в кластер балансировки

По умолчанию в кластере балансировки активен только первый узел фильтрации, поэтому остальные узлы необходимо активировать. Для этого необходимо нажать на соответствующую строку узла фильтрации, после чего с правой стороны появится дополнительное окно с информации о выбранном узле фильтрации (Рисунок 51). Далее необходимо перейти в режим редактирования путем нажатия пиктограммы , нажать на переключатель Active , после чего он станет зеленым, а также указать вес узла в кластере балансировки (чем больше вес – тем больше трафика будет обрабатывать узел фильтрации, для режимов «rr» и «lc» неприменимо). В случае указания значения «0» - данный узел не будет участвовать в балансировке нагрузки.

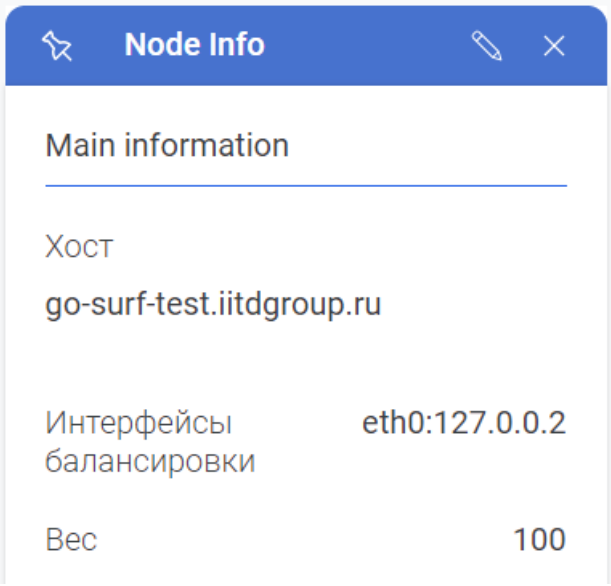


Рисунок 51 – Информация об узле балансировки нагрузки

Если существует необходимость корректировки параметров кластера балансировки, то для этого необходимо нажать на имя кластера в левой части интерфейса, после чего будет отображено окно со сводной информацией в правой части экрана. Для редактирования параметров необходимо нажать пиктограмму .

Допускается создание нескольких кластеров балансировки нагрузки, основным условием корректной работы – для всех кластеров должны быть использованы уникальные виртуальные IP адреса.

Удаление узла фильтрации из кластера балансировки осуществляется путем выставление отметки в поле ☐ слева от имени узла, после чего появится пиктограмма Исключить , нажатие на которую приведет к удалению узла фильтрации.

Для удаления кластера балансировки целиком, необходимо в левой части меню (Рисунок 52) нажать на строку с именем кластера балансировки у нажать пиктограмму Delete , после чего подтвердить действие во всплывающем меню.

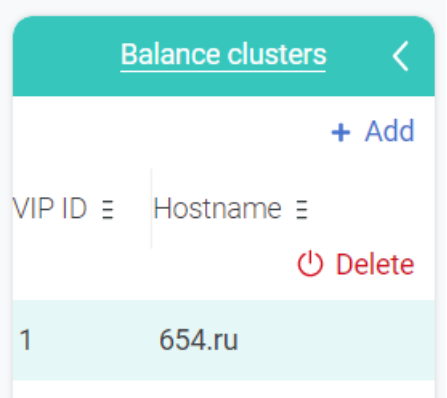


Рисунок 52 – Информация о существующих кластерах балансировки

### 3.10.3 Управление лицензиями

Инструменты управления кластера содержат в себе дополнительные возможности по централизованному управлению лицензиями всех узлов, входящих в кластер конфигурации. Инструменты по просмотру и настройки лицензий расположены в разделе «Кластера» в меню «License management» (Рисунок 53).

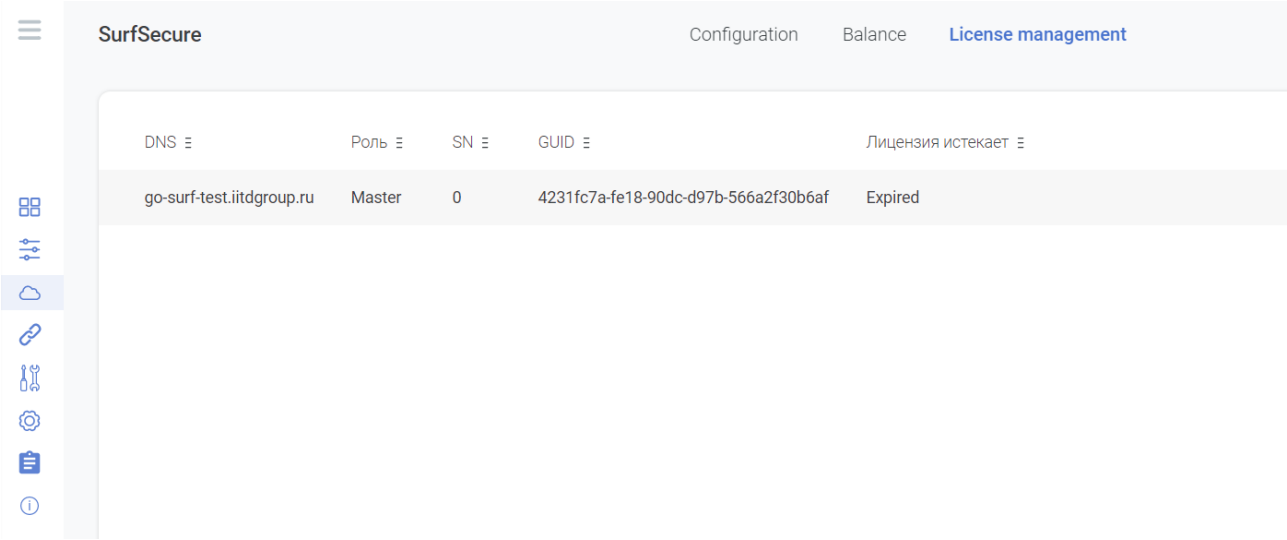


Рисунок 53 – Интерфейс централизованного управлениями лицензиями узлов кластера

Данный инструмент полностью копирует локальный интерфейс управления лицензиями на каждом узле фильтрации и создан для удобства обслуживания кластера. Просмотр информации и активации новых лицензий может осуществляться как через локальный интерфейс узла фильтрации (см. п. 3.14), так и через интерфейс управления кластером.

Данный интерфейс отображает весь перечень узлов, которые входит в кластер, и информацию об установленной лицензии. Для активации новой лицензии необходимо нажать на строку с нужным узлом фильтрации, в результате чего отобразится дополнительное окно с параметрами активации новой лицензии. Активация лицензии осуществляется аналогично процессу активации через локальный интерфейс, возможные варианты и необходимые действия отражены в разделе п. 3.14.

## 3.11 Контроль доступа

Настройка политик доступа пользователей к ресурсам сети интернет, объектов доступа и исключений осуществляется в разделе «Контроль доступа» (Рисунок 54).

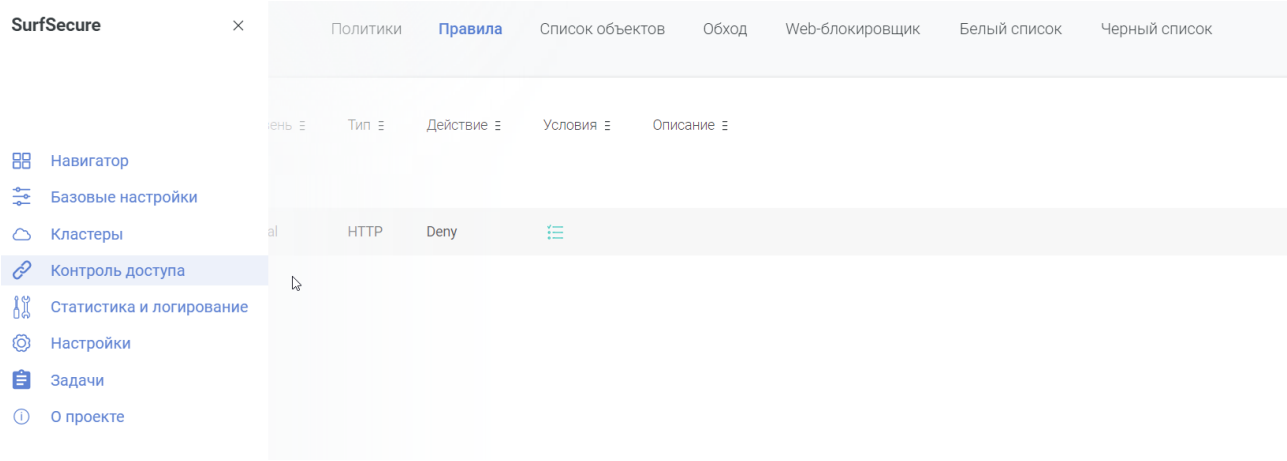


Рисунок 54 – Раздел контроль доступа

В системе присутствуют три глобальных списков доступа:

- Политики;

- Черный список;
- Белый список.

Очередность их применения указывается в разделе «Базовые настройки», меню «Системные настройки», пункт «Правила» (Рисунок 55).

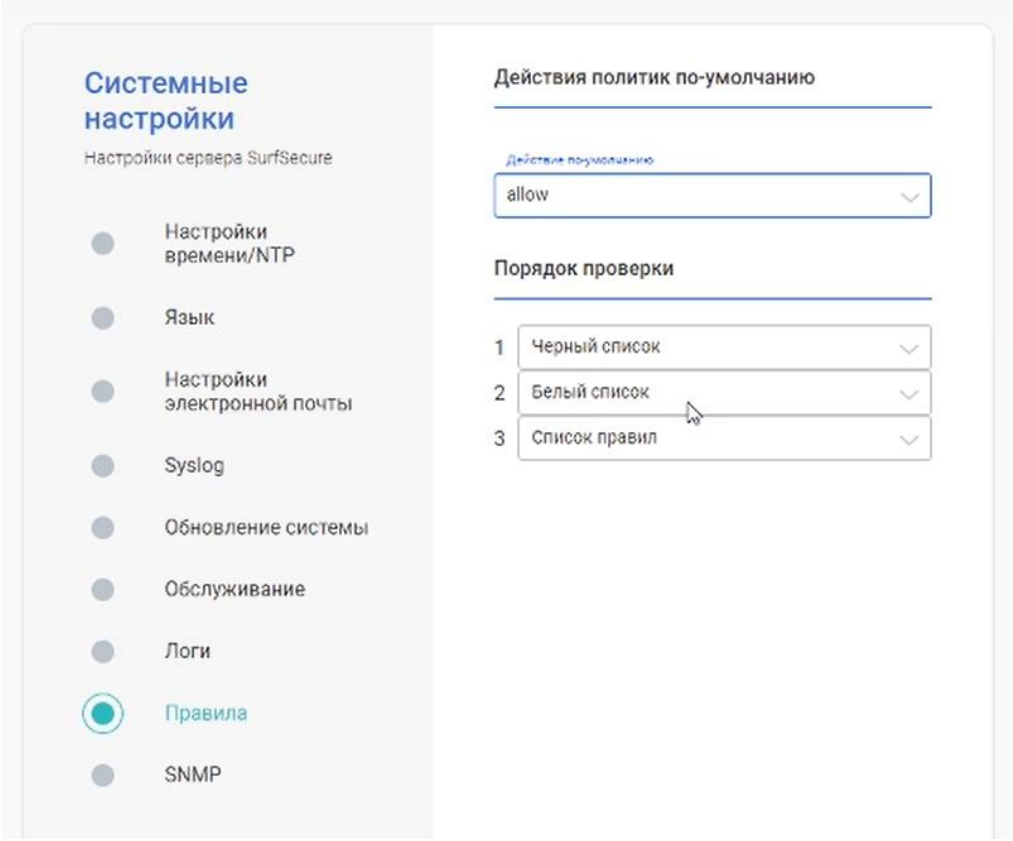


Рисунок 55 – Порядок применения списков фильтрации

Также необходимо указать «Действие по умолчанию», которое будет применяется, в случае если запрос пользователя не соответствует ни одному списку доступа.

Черные и белые списки применяются автоматически на всех пользователей, в то время, как политики доступа могут быть применены только к:

- Пользователю;
- Группе пользователей (в т.ч. поддерживается вложенность групп);
- Всем пользователям (глобальная политика).

Настройка политик доступа подробно описана в разделе 3.11.2.

Все списки доступа формируются на основании объектов (URL, IP адреса и т.д.), поэтому первым шагом при создании списка доступа это создание объектов. Система позволяет делать как отдельные объекты (например конкретный URL), так и списки объектов, который будет состоять из нескольких отдельных объектов (например перечень URL связанных одной тематикой). Настройка объектов доступа подробно описана в разделе 3.11.1

### 3.11.1 Объекты и списки

Для редактирования объектов списков доступа необходимо перейти в меню «Список объектов» раздела «Контроль доступа» (Рисунок 56).

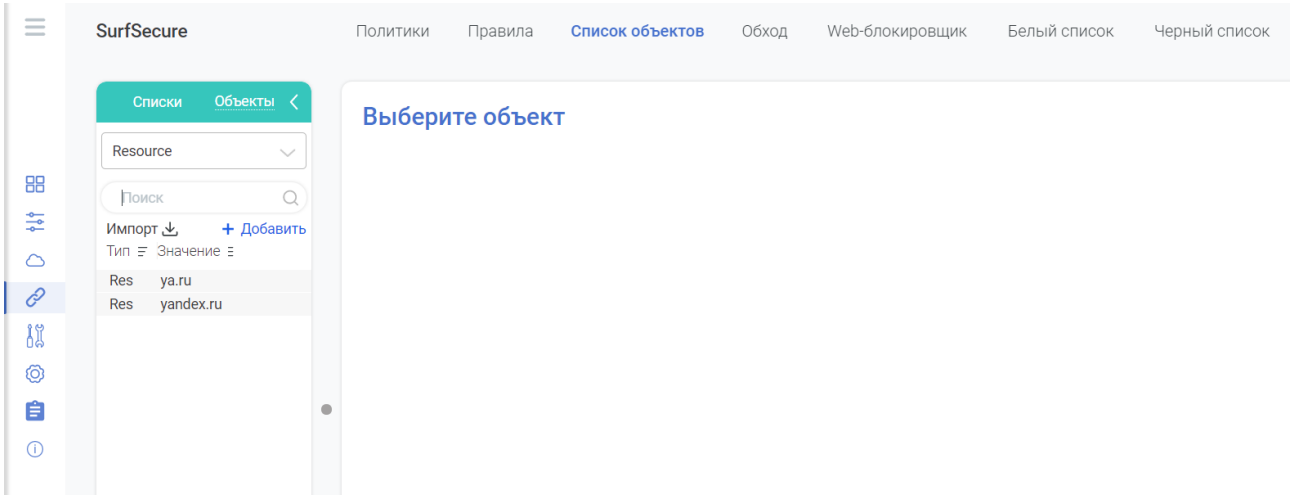


Рисунок 56 – Интерфейс конфигурации объектов и списков объектов

В данном разделе возможно создать объекты доступа, а также впоследствии объединять их в списки объектов, которые затем можно использовать в политиках доступа для удобства. Переключение между меню работы с объектами и списками объектов осуществляется за счет выбора необходимого подменю (Рисунок 57).

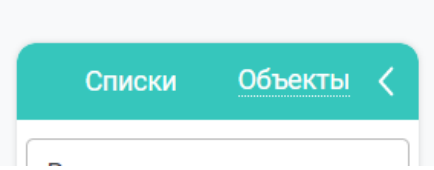


Рисунок 57 – Изменение режимов работы с объектами

Для удобства работы с именами объектов и списков возможно изменение ширины области отображения, которое осуществляется за счет перетягивания пиктограммы влево или вправо для изменения ширины.

#### 3.11.1.1 Объекты

Для создания объекта необходимо в выпадающем меню выбрать тип объекта и нажать кнопку «Добавить» (Рисунок 58).

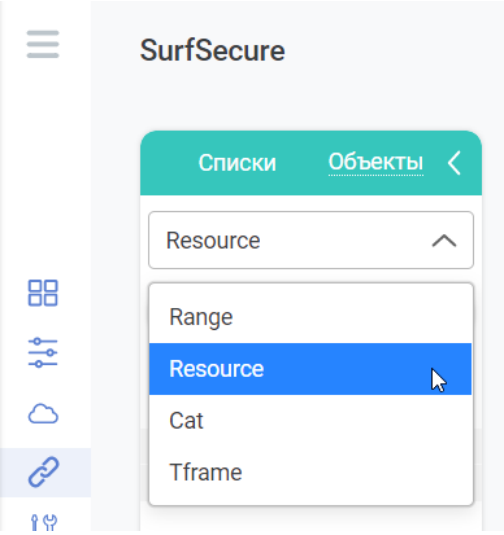


Рисунок 58 – Выбор типа объекта

После выбора типа объекта с правой стороны окна отобразится окно для его настройки. Система содержит в себе следующие типы объектов:

- Range – Диапазон IP адресов. Указывается в формате CIDR 1.2.3.4/24. Для задания единственного IP адреса необходимо указать маску «/32»;

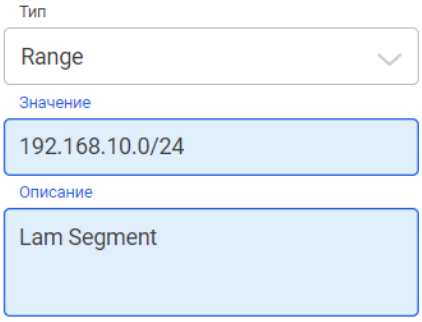


Рисунок 59 – Создание объекта типа Range

- Resource – Указывается домен, конкретный URL (например - ya.ru/index.php) или ip адрес веб ресурса (рассматривается как URL). Допускается указывать «.» как регулярное выражение. Например «.yandex.» означает, что в это объект будет входить любой URL, который содержит сочетания «yandex»;

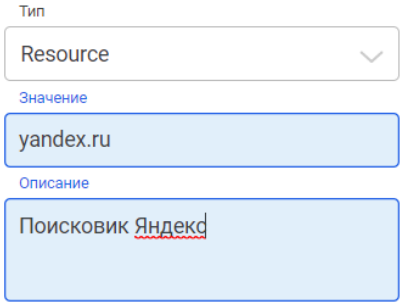


Рисунок 60 – Создание объекта типа Resource

- Cat – категории веб ресурсов. E1 и e2 – указан тип механизма, который содержит данный тип категорий. Данные объекты поставляются и обновляются производителем, их редактирование или добавление невозможно;
- App – предустановленные производителем сигнатуры трафика определенных приложений для их распознавания и формирования политик доступа на основе используемого пользователем приложения;
- Timeframe – промежуток времени, в которое будет действовать правило. Необходимо указать время начала и конца диапазона, а также дни недели. Время начала временного диапазона должно быть раньше времени его окончания.


Рисунок 61 – Создание объекта типа

По окончанию настройки параметров объекта необходимо нажать «Создать», после чего объект появится в общем перечне объектов.

Для редактирования созданного объекта необходимо нажать на имя объекта, после чего в правой стороне окна нажать пиктограмму  и по окончанию внесения изменений нажать «Save object». При необходимости, возможно создание копии объекта за счет кнопки  . Удаление объекта осуществляться за счет нажатия на имя объекта и кнопки 

.

### 3.11.1.1 Списки объектов

Для создания списка объектов необходимо выбрать подменю «Списки» и нажать кнопку «Добавить список» (Рисунок 62).

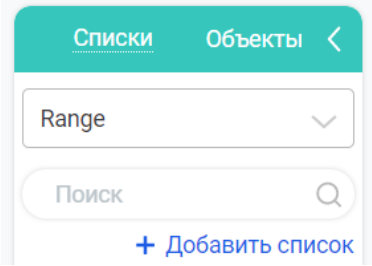


Рисунок 62 – Создание списка объектов

В правой части интерфейса отобразится окно для ввода параметров нового списка объектов (Рисунок 63).

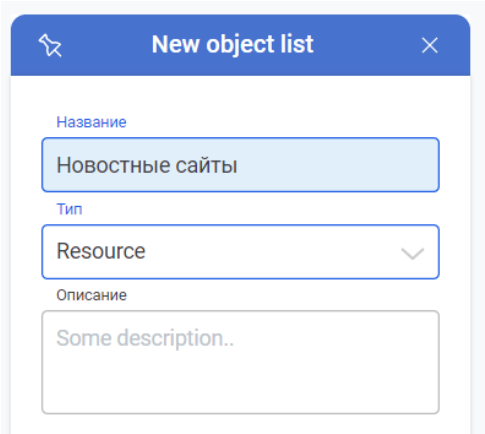


Рисунок 63 – Конфигурация параметров списка объектов

Необходимо ввести уникальное имя списка (вне зависимости от типа) и выбрать тип объектов, которые нужно объединить. Система позволяет создавать списки объектов следующих типов:

- Range - список диапазонов IP адресов;
- Resource – список URL и доменов ресурсов;
- Cat – список категорий;
- APP – список приложений.

Указание описания списка опционально и может быть использовано как информационное поле для администратора системы. Далее нажать кнопку «Create object list» для создания списка.

Для добавления объектов в список необходимо нажать на имя списка в левой части интерфейса, после чего отобразиться информационной окно о данном списке в правой части. Вход в режим редактирования осуществляется кнопкой «Manage» в правой нижней части интерфейса, по нажатию на которую открывается интерфейс добавления объектов в список (Рисунок 64).

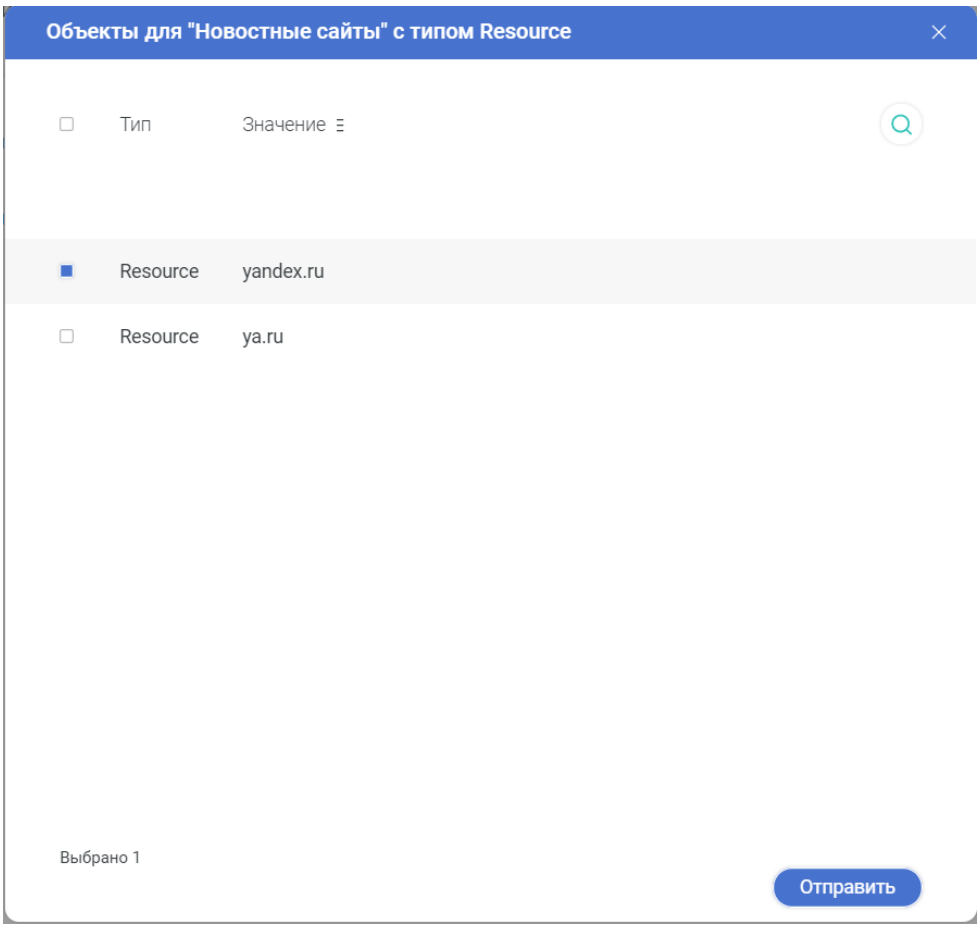


Рисунок 64 – Добавление объектов с список

Далее в зависимости от типа списка будут предложены ранее созданные объекты для добавления. Чтобы включить объект в список нужно поставить отметку ■ напротив имени объекта и нажать кнопку «Отправить».

Для всех списков объектов должны задаваться уникальные имена вне зависимости от типа.

При нажатии на имя списка в левой части экрана будут отображены все объекты, которые в него входят (Рисунок 65).

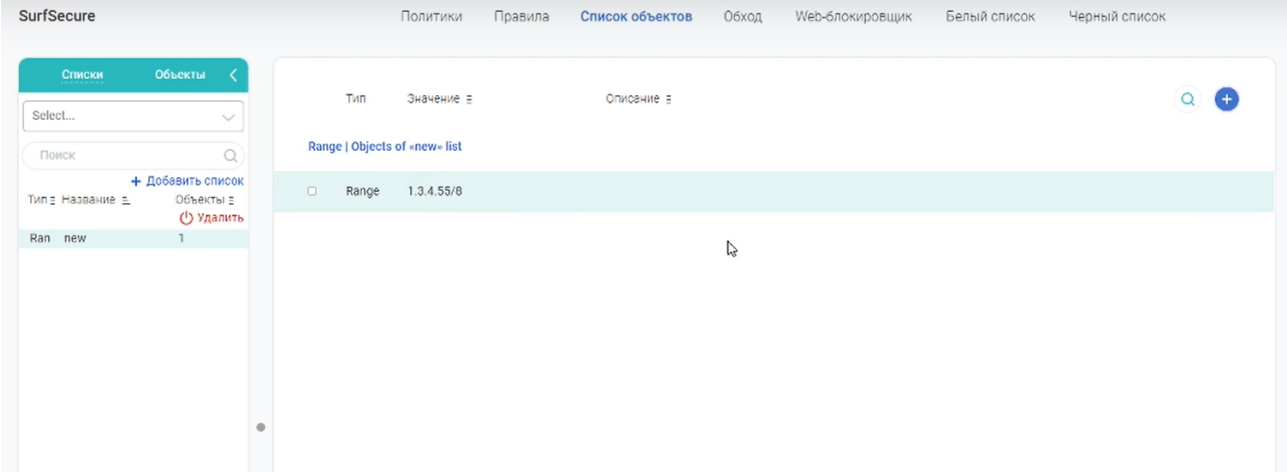


Рисунок 65 – Просмотр информации о созданном списке

В меню работы со списками существует возможность создавать и автоматически добавлять объекты в список. Для этого необходимо нажать , после чего в правой части экрана отобразиться интерфейс создания объекта такого же типа, как и список. По окончанию ввода информации для нового объекта необходимо нажать кнопку «Create object» для сохранения настроек.

Если список объектов уже используется в правилах и в данный список вносятся изменения, то отобразиться всплывающее окно с перечнем политик, где данный список применен (Рисунок 66). В данном окне необходимо указать для каждого правила, будет ли включен новый объект в зону действия или нет, после чего нажать «Применить».

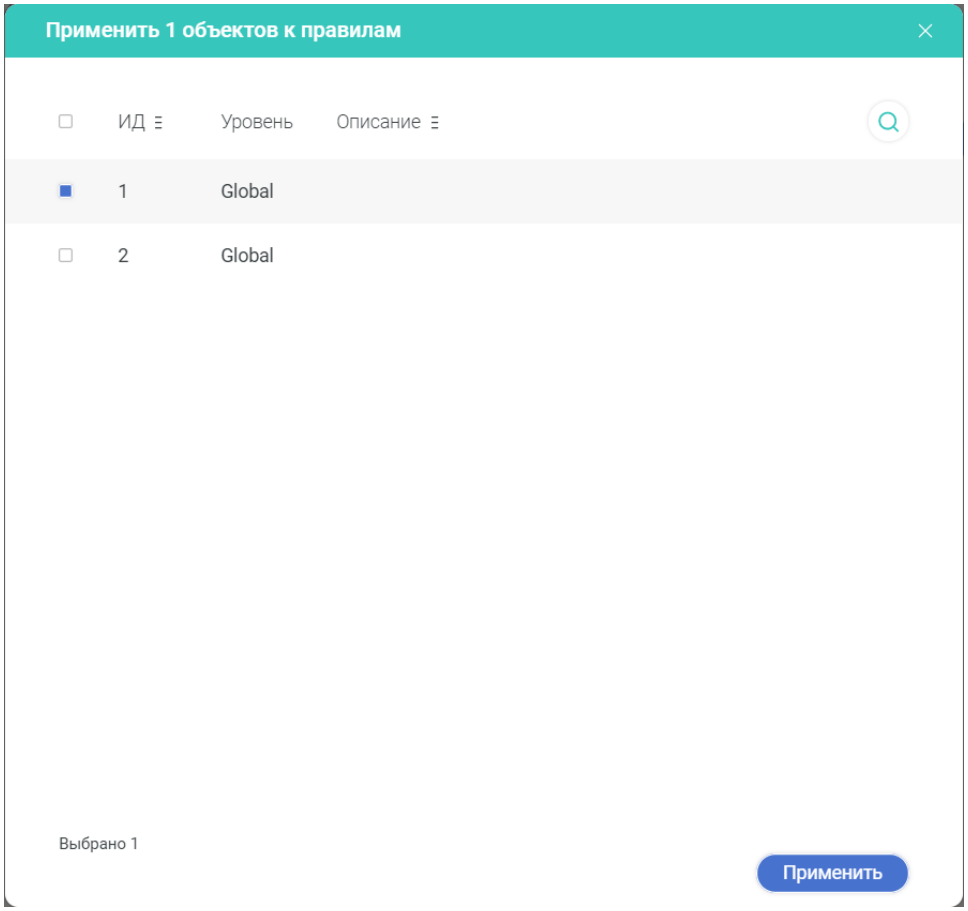


Рисунок 66 – Окно уведомление об изменении

### 3.11.2 Политики

Политики представляют собой правила доступа, которые привязаны к определённому субъекту доступа, благодаря такой связке система и осуществляет контроль доступа пользователей в сеть интернет. Правила содержат набор критериев, под которые должен попасть запрос пользователя, а также действие, которое будет выполнятся с данным запросом.

Применение политик работает по признаку первого совпадения с запрашиваемым ресурсом, отрабатывает только одна политика и дальнейшая обработка запроса пользователя не осуществляется. Если запросу пользователя не соответствует ни одна политика, то к такому запросу применяется действие по умолчанию, которое задается в

системных настройках политик (см. п.3.11). В этом же меню задается очередность применения политик, черных и белых списков.

Существует несколько видов правил доступа:

- Глобальные – применяются на всех пользователей, вне зависимости от вхождения пользователя в доменную группу пользователей или его имени;
- Групповые – применяются к доменной группе пользователей. Вложенность групп поддерживается;
- Пользовательские – применяются к конкретному доменному пользователю.

При фильтрации запроса пользователя правила доступа будут применены в следующем порядке:

- Пользовательские;
- Групповые;
- Глобальные.

Если для пользователя не создано персональное правило, то будут применяется правила доступа для доменных групп, в которые входит данный пользователь. Если для групп также не создано правил, то будут применяться глобальные правила доступа, а в случае отсутствие совпадения с глобальными правилами – действие по умолчанию.

Работа с политиками доступа осуществляется в разделе «Контроль доступа» в меню «Политики» (Рисунок 67).

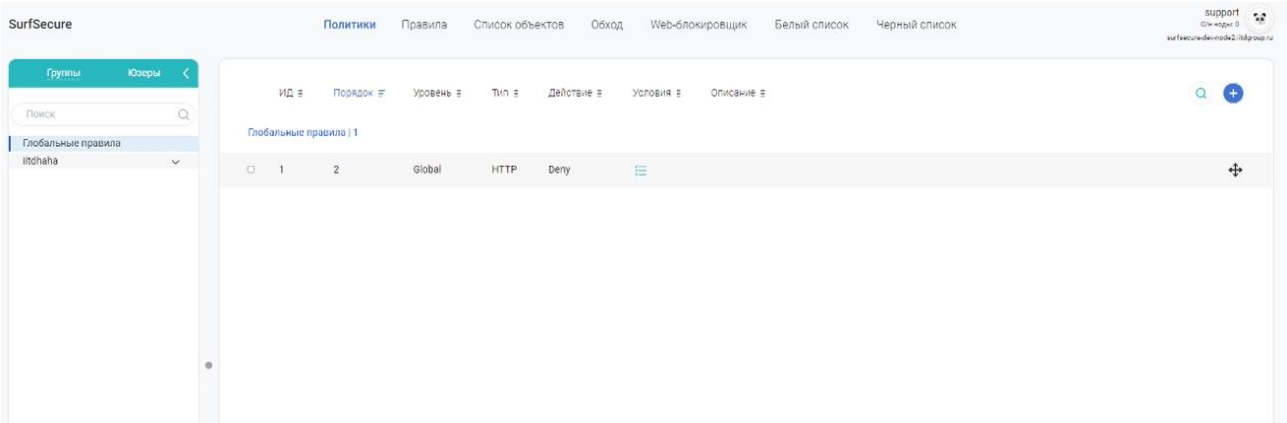


Рисунок 67 – Интерфейс работы с политиками доступа

Создание всех видов правил доступа идентично, поэтому создание политики доступа будет рассмотрено на примере глобального правила и далее в инструкции будут рассмотрены способы создания остальных видов правил.

Для создания глобального правила необходимо в левой части экрана нажать на список «Глобальные правила», в результате чего в центральной области интерфейса отобразится весь перечень ранее созданных правил. Для создания правила необходимо нажать на пиктограмму  , после чего в правой части интерфейса отобразится базовое меню для указания параметров (Рисунок 68).


Рисунок 68 – Создание правила доступа

Для каждого создаваемого правила нужно указать:

- Действие, которое будет выполнено:
  - Allow – разрешить запрос;
  - Deny – заблокировать запрос;
- Тип трафика:
  - **HTTP** – правило будет применятся на основе списков ресурсов и\или их категорий. В таком случае необходимо задать следующие критерии:
    - Объекты назначения:
      - Любой – будет применяться вне зависимости от URL, домена или IP адреса ресурса назначения;
      - Созданный список объектов типа Resource (может использоваться только один список);
    - Категории:
      - Любой – будет применяться вне зависимости от категории запрашиваемого ресурса;
      - Созданный список объектов типа Cat (может использоваться только один список);
  - **AI** – правило будет применяться на основе IP адресов источника и\или типа приложения, которое установлено у пользователя (мессенджеры, приложения социальных сетей и т.д.). В таком случае необходимо задать следующие критерии:
    - Объекты назначения:
      - Любой – будет применяться вне зависимости IP адреса источника запроса;
      - Созданный список объектов типа Range (может использоваться только один список);
    - Приложения:
      - Любой – будет применяться вне зависимости от типа приложения;
      - Созданный список объектов типа App (может использоваться только один список).

В том случае, если будет указано значение «Любой» для всех параметров – правило доступа будет срабатывать всегда. При выборе какого-либо списка объектов, по умолчанию используются все объекты из данного списка. При необходимости, существует возможность исключить некоторые объекты из выбранного списка, таким образом правило не будет применяться при обращении к исключенным объектам. Для этого необходимо нажать на пиктограмму ⌄ у выбранного списка, в результате чего будут отображены все объекты, входящие в данный список. Для добавления или исключения конкретного объекта необходимо нажать на пиктограмму ■ напротив наименования объекта (Рисунок 69).

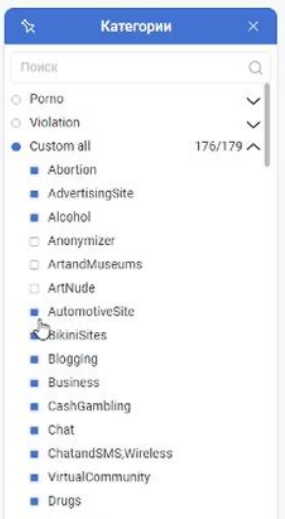


Рисунок 69 – Выбор списка объектов

При создании правила доступа существует возможность указать ряд дополнительных настроек. Для этого, при создании правила доступа, необходимо нажать на ссылку «Расширенные настройки», в результате чего отобразятся дополнительные поля, которые являются необязательными:

- Объект источника – выбор диапазона IP адресов источников запросов, т.е. IP адреса АРМ пользователя. В качестве значения необходимо указать список объектов типа Range;
- TimeFrame – временной интервал, в который данное правило будет активно. В качестве значения необходимо указать объект типа TimeFrame;
- File Types – типы файлов (категории или конкретные расширения). Выбирается из предустановленных списков, допускается выбор нескольких списков;
- Методы – HTTP методы, к которым будем применено правило;
- Размер файла – ограничение на размер скачиваемого файла, указывается в мегабайтах.

По окончанию ввода необходимых параметров необходимо нажать на кнопку «Создать правило» для сохранения правила.

Для создания других видов правил доступа необходимо в меню «Политики» выбрать группу пользователей или конкретного пользователя и создать для выбранного объекта новое правило. Выбор групп и пользователей осуществляется в левой части интерфейса, для этого необходимо выбрать нужную вкладку в верхнем меню «Группы\Юзеры». Далее в списке

будет отображено наименование LDAP коннектора, раскрыв который будет отображен полный перечень пользователей или групп (Рисунок 70).

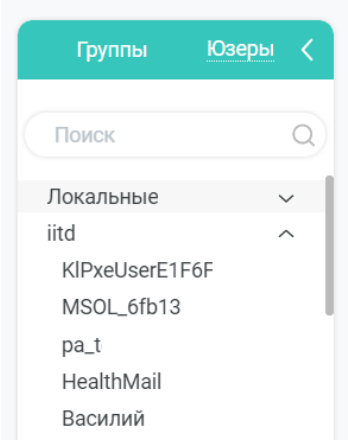


Рисунок 70 – Перечень доменных пользователей

Следующим шагом необходимо выбрать пользователя или группу и нажать пиктограмму для создания правила, действия по его созданию описаны ранее в данном разделе.

В основном интерфейсе работе с политиками при нажатии на пользователя или группу пользователей будет отображен тот перечень правил доступа, который будет применен (Рисунок 71).

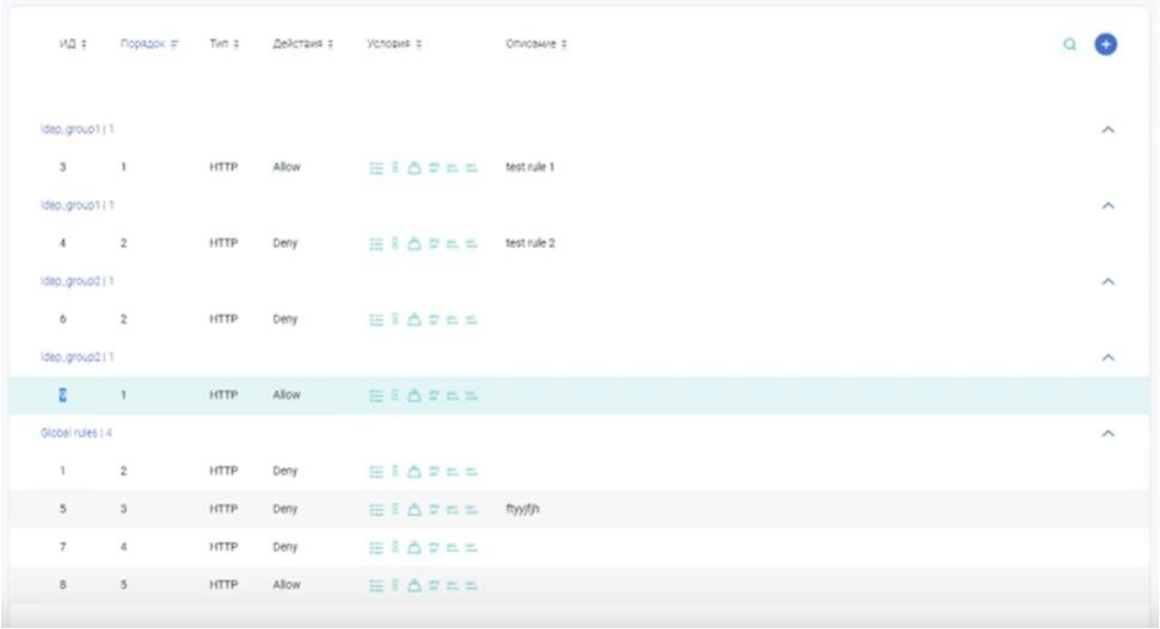


Рисунок 71 – Отображение перечня правил для пользователя

При создании нескольких глобальных правил или создании нескольких правил доступа для группы или пользователя – данные правила будут применяться, начиная с самого верхнего в списке. Для изменения порядка применения необходимо использовать пиктограмму и осуществить изменения порядка правил путем их перетаскивания.

Чтобы временно приостановить действие правила и сохранить настройки самого правила возможна его деактивация. Для этого необходимо установить отметку ■ напротив выбранного правила и в появившемся подменю нажать кнопку «Деактивировать», после чего строка с выбранным правилом станет серой. Для удаления правила нужно выбрать его аналогичным способом и нажать кнопку «Удалить» (Рисунок 72).

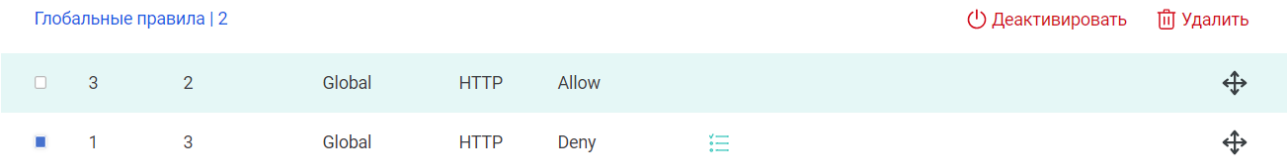


Рисунок 72 – Деактивация и удаление правил доступа

### 3.11.3 Правила

Весь перечень созданных правил доступа отображается в разделе «Контроль доступа» в меню «Правила» (Рисунок 73). Данное меню создано для удобной работы с созданными правилами доступа, а также исключает необходимости поиска группы или пользователя для редактирования правил, которые к ним применяются.

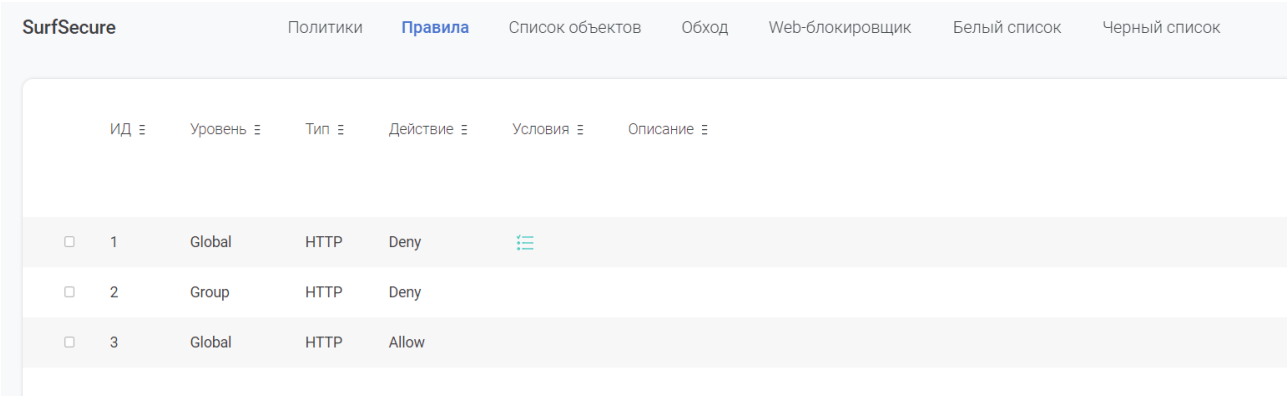


Рисунок 73 – Общий перечень правил доступа

Интерфейс работы с правилами доступа отображает следующие характеристики для каждого правила:

- ИД – уникальный идентификатор правила;
- Уровень – отображает тип правила (глобальное, групповое или пользовательское);
- Тип – отображает выбранный тип обработки трафика (HTTP или AI);
- Действие – применяемое действие (Allow или Deny);
- Условия – отображается пиктограммы критериев, которые были заданы в правиле доступа:
  - DST - Указаны объекты назначения;
  - - Указаны категории веб ресурсов;
  - - Указан максимальный размер файла;

- - Указан параметр тип файлов;
- - Указан объект источника;
- - Указан временной интервал.

- Описание – отображение заданного описания правила доступа.

При нажатии на конкретное правило доступа, в правой части экрана отобразится сводная информация по заданным параметрам данного правила (Рисунок 74).

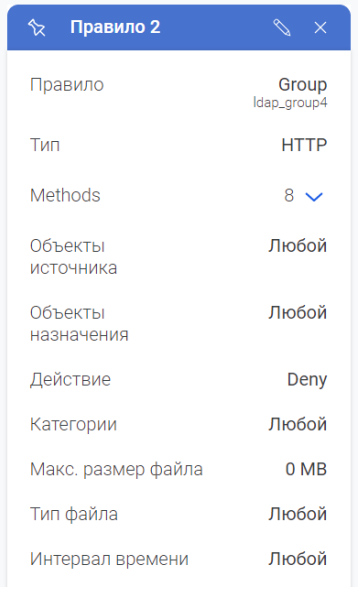


Рисунок 74 – Сводная информация о параметрах правила доступа

Для быстрого редактирования правила необходимо нажать на пиктограмму .

### 3.11.4 Обход

Меню обход предназначено для задания исключений при обработке системой пользовательского трафика. Для перехода в интерфейс работы с исключениями необходимо перейти в раздел «Контроль доступа» и выбрать меню «Обход» (Рисунок 75).

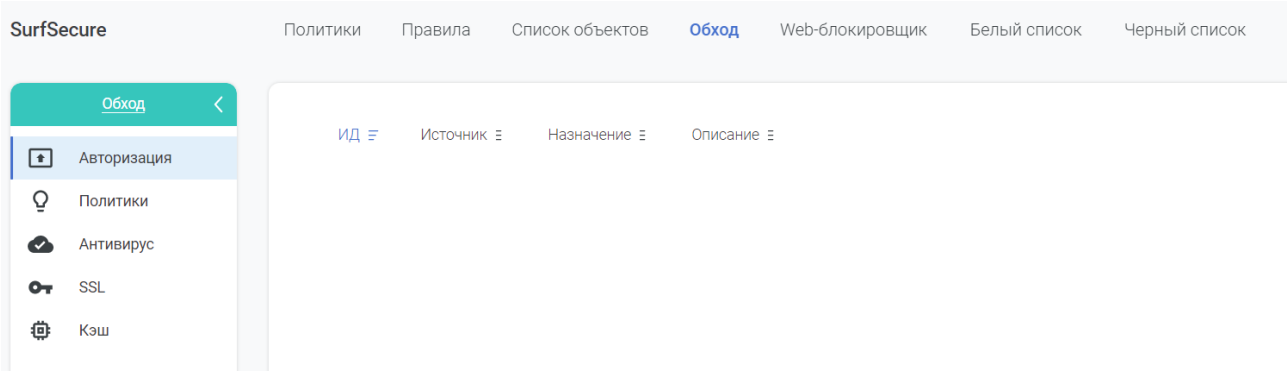


Рисунок 75 – Интерфейс работы с исключениями

Система предусматривает создание следующих типов исключений:

- Авторизация;

- Политики;
- Антивирус;
- SSL;
- Кэш.

**Исключение типа авторизация** позволяет исключить процесс аутентификации пользователя. В таком случае к запросу будут применены только глобальные правила и черные\белые списки. Данное исключение может быть применено, когда у компании нет каталога доменов или LDAP-каталога, а также может быть использовано для работы ПО, которое не поддерживает работу с прокси серверам. Для создания данного исключения необходимо задать один или несколько из следующих параметров:

- Объекты назначения – списки объектов типа Range и Resource;
- Объекты источника – список типа Range.

**Исключение типа политики** позволяет отключить обработку запросов политиками доступа. Для создания данного исключения необходимо задать один или несколько из следующих параметров:

- Объекты назначения – списки объектов типа Range и Resource;
- Объекты источника – список типа Range.

**Исключение типа антивирус** позволяет отключить обработку запросов антивирусным механизмом. Для создания данного исключения необходимо задать один или несколько из следующих параметров:

- Объекты назначения – списки объектов типа Range и Resource;
- Объекты источника – список типа Range;
- Типы файлов – выбор из списка предустановленных.

**Исключение типа SSL** позволяет отключить обработку запросов механизмом разбора SSL трафика или изменить его действие. Для создания данного исключения необходимо задать один или несколько из следующих параметров:

- Объекты назначения – списки объектов типа Range и Resource;
- Объекты источника – список типа Range.

Дополнительно необходимо выбрать как данное исключение будет отработано механизмом разбора SSL трафика:

- Bypass – трафик будет пропущен без разбора и подмены сертификатов;
- Fix Expired – в случае, если сертификат запрашиваемого ресурса просрочен, данная опция позволяет это скорректировать - пользователю не будет выдаваться предупреждающее сообщение;
- Fix Not Yet Valid - в случае, если сертификат запрашиваемого ресурса еще не начал действовать, данная опция позволяет это скорректировать - пользователю не будет выдаваться предупреждающее сообщение;
- Fix Domain Mismatch - в случае, если сертификат не соответствует доменному имени или url запрашиваемого ресурса, данная опция позволяет это

скорректировать - пользователю не будет выдаваться предупреждающее сообщение;

- Fix Untrusted - в случае, если сертификат запрашиваемого ресурса выпущен недоверенным центром сертификации, данная опция позволяет это скорректировать - пользователю не будет выдаваться предупреждающее сообщение;
- Fix Self Signed - в случае, если запрашиваемый ресурс использует самоподписанный сертификат, к которому отсутствует доверие, данная опция позволяет это скорректировать - пользователю не будет выдаваться предупреждающее сообщение.

**Исключение типа кэш** позволяет исключить из кэширования файлы, которые передаются при работе с веб ресурсами, в т.ч. элементы самих веб страниц. Для создания данного исключения необходимо задать один или несколько из следующих параметров:

- Объекты назначения – списки объектов типа Range и Resource;
- Объекты источника – список типа Range;
- Типы файлов – выбор из списка предустановленных.

### 3.11.5 Черные списки

Черные списки предназначены для блокировки доступа пользователей к определенным ресурсам. Интерфейс работы с черными списками расположен в разделе «Контроль доступа» в меню «Черный список» (Рисунок 76).

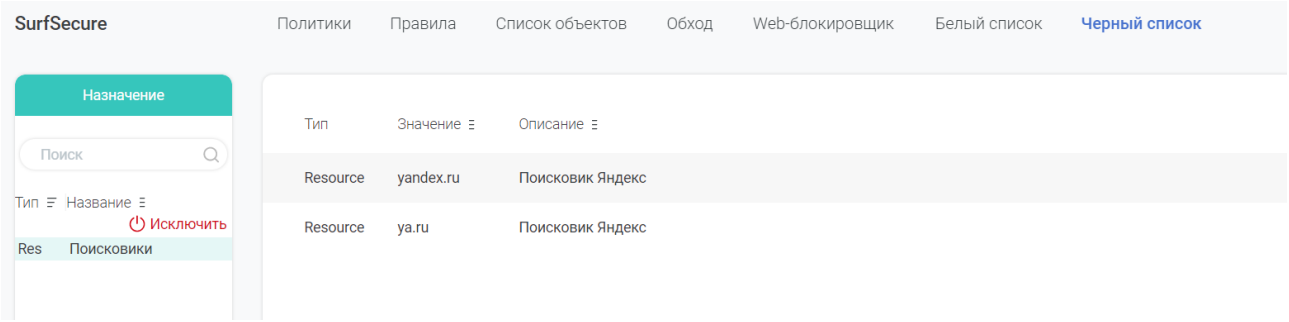


Рисунок 76 – Интерфейс настройки черных списков

В черный список допускается добавление только списка объектов типа Resource, причем будет добавлены все объекты списка. Для добавления списка в левой части интерфейса необходимо нажать на кнопку «Добавить списки», выбрать необходимые и нажать кнопку «Сохранить». Для удаления списка необходимо в левой части интерфейса выбрать нужный список и нажать на кнопку «Исключить».

В случае добавления одного и того же списка объектов в черный и белый список, обработка запроса будет осуществляться в порядке применения правил, который указан в базовых системных настройках (см. п. 3.11).

### 3.11.6 Белые списки

Белые списки предназначены для разрешения доступа пользователей к определенным ресурсам. Интерфейс работы с белыми списками расположен в разделе «Контроль доступа» в меню «Белый список» (Рисунок 77 – Интерфейс настройки белых списков).

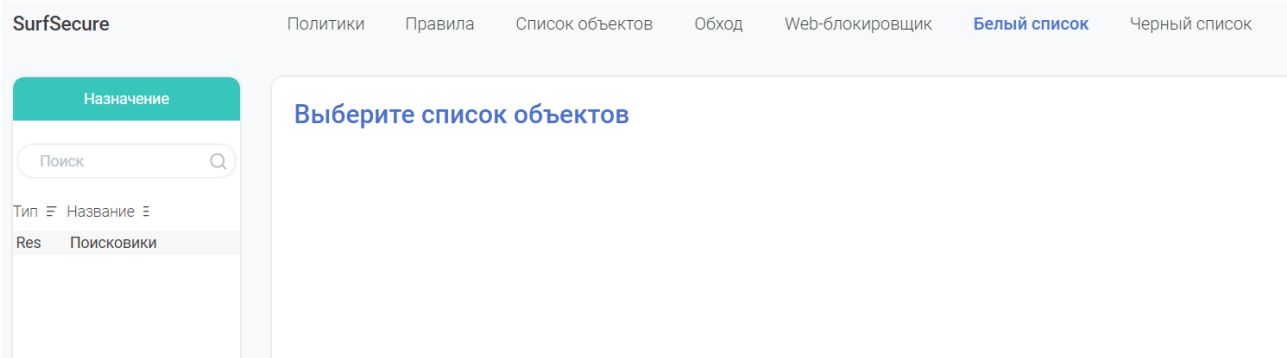


Рисунок 77 – Интерфейс настройки белых списков

В белый список допускается добавление только списка объектов типа Resource, причем будет добавлены все объекты списка. Для добавления списка в левой части интерфейса необходимо нажать на кнопку «Добавить списки», выбрать необходимые и нажать кнопку «Сохранить». Для удаления списка необходимо в левой части интерфейса выбрать нужный список и нажать на кнопку «Исключить».

В случае добавления одного и того же списка объектов в черный и белый список, обработка запроса будет осуществляться в порядке применения правил, который указан в базовых системных настройках (см. п. 3.11).

### 3.11.7 Web-блокировщик

В случае если запрос пользователя заблокирован системой, ему будет отображено уведомление о его блокировке. Данный интерфейс обеспечивает возможность редактирования данного уведомления (Рисунок 78).

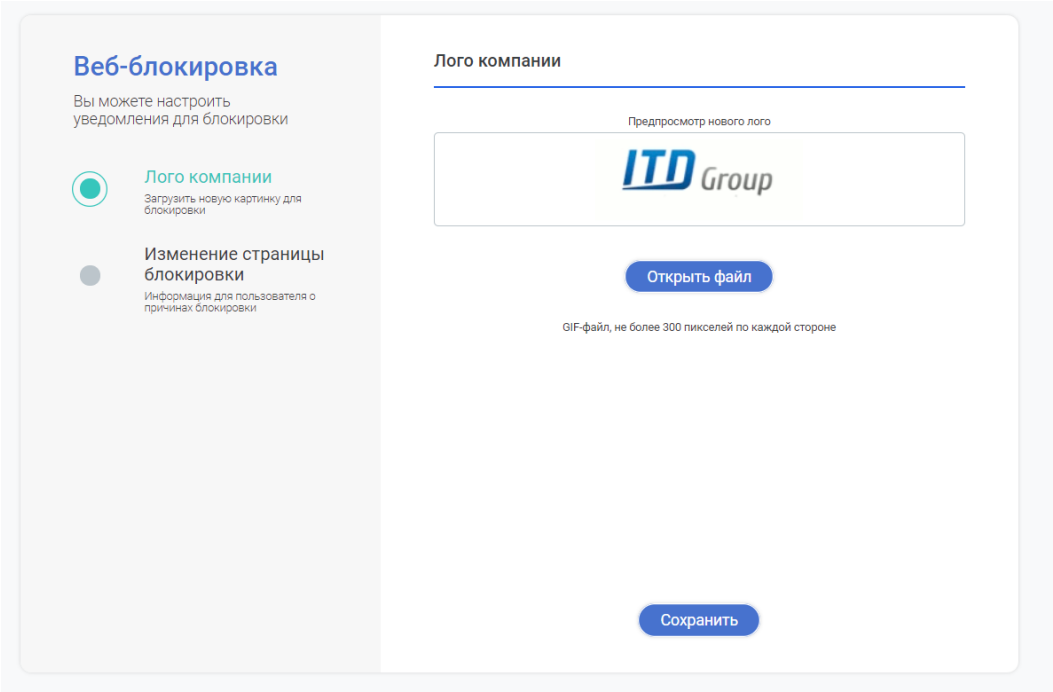


Рисунок 78 – Интерфейс настройки уведомления о блокировке

В левой части меню присутствуют две вкладки:

- Лого компании;
- Изменение страницы блокировки.

Загрузка собственного логотипа осуществляется во вкладке «Лого компании», для этого необходимо нажать кнопку «Открыть файл», выбрать необходимое изображение и нажать кнопку «Сохранить». Требование к файлу логотипа следующие:

- Формат – GIF;
- Ширина – не более 300 пикселей;
- Высота – не более 300 пикселей.

Для изменения содержания страницы блокировки необходимо перейти в меню «Изменение страницы блокировки» (Рисунок 79).

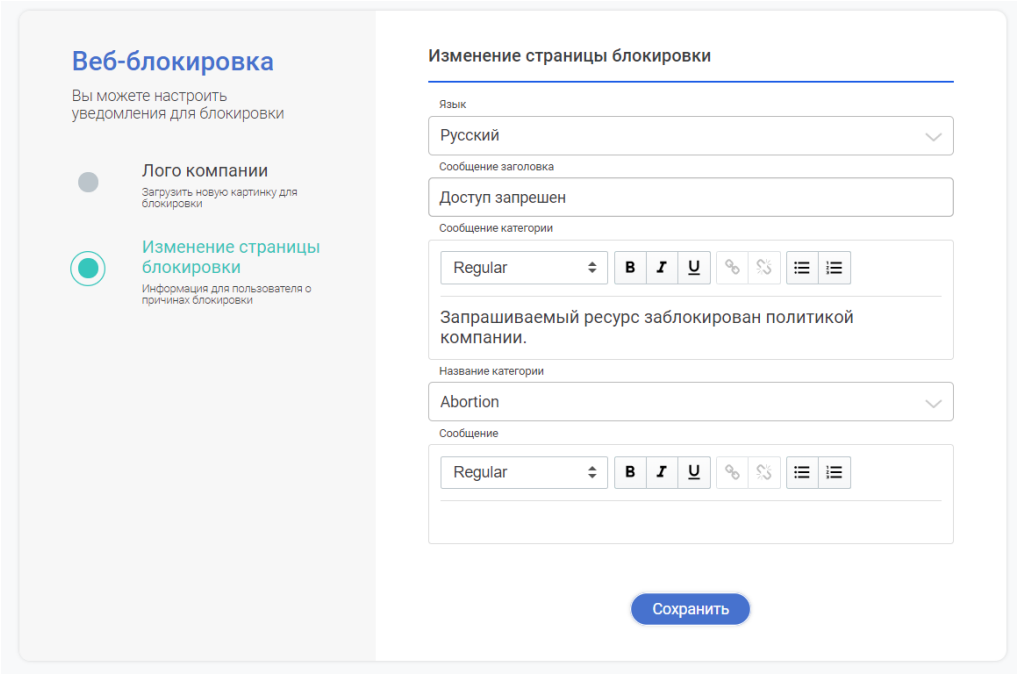


Рисунок 79 – Изменение содержания страницы блокировки

Здесь возможно скорректировать следующие параметры:

- Язык – предустановленные шаблоны оповещения на русском или английском языках;
- Сообщение заголовка – корректировка заголовка веб страницы;
- Сообщение – основной текст уведомления;

Дополнительно для каждой категории веб ресурсов возможно указать дополнительную индивидуальную информацию, например, причины блокировки материалов того или иного характера. Для этого нужно выбрать необходимую категорию в выпадающем списке «Название категории» и в графе «Сообщение» указать дополнительную информацию. Для сохранения настроек необходимо нажать кнопку «Сохранить».

## 3.12 Резервное копирование системы

Система имеет функционал резервного копирования конфигурации системы для обеспечения возможности восстановления настроек узла фильтрации. Инструменты работы с данным функционалом находятся в разделе «Базовые настройки» в меню «Бэкап» (Рисунок 80).

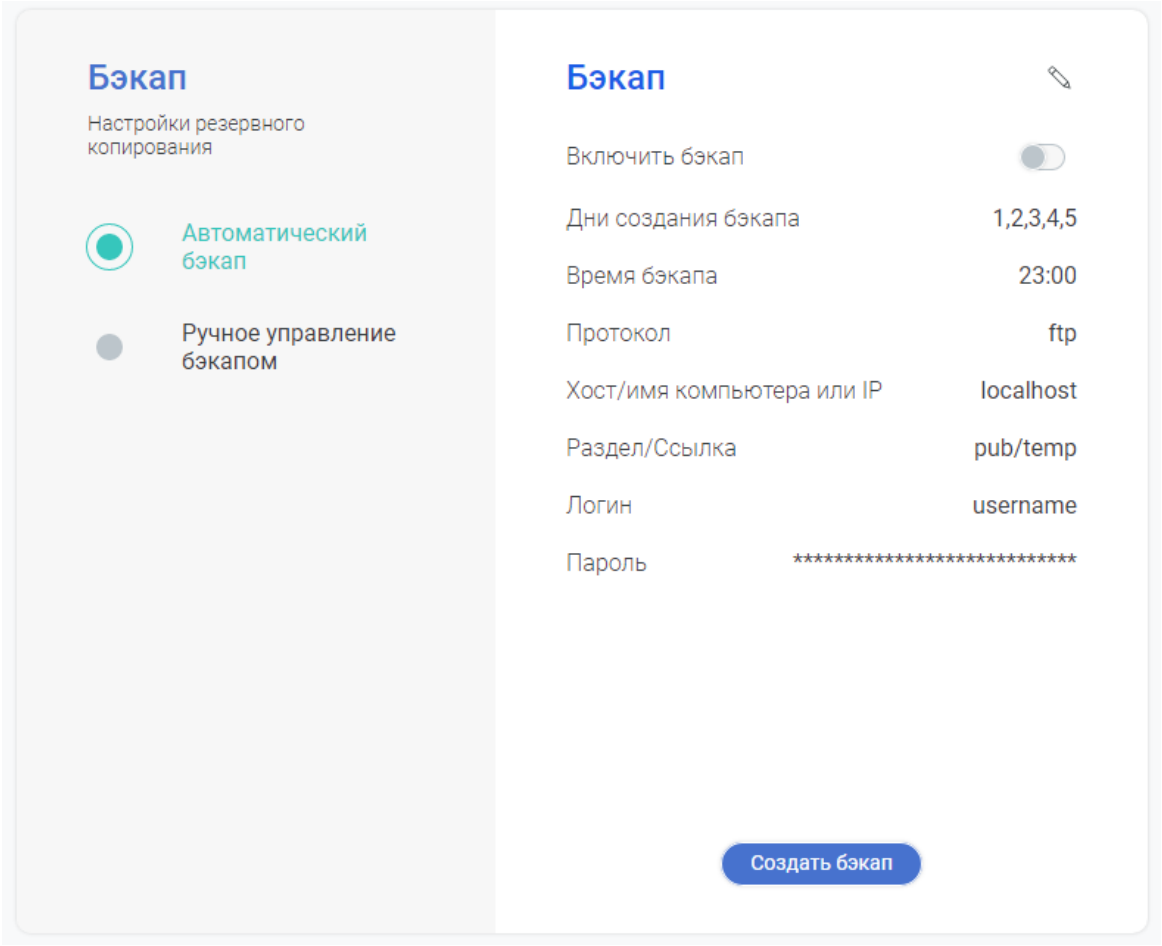


Рисунок 80 – Интерфейс настройки механизма резервного копирования

Инструменты системы позволяют осуществлять создание резервное копирование конфигурации узла фильтрации в следующих режимах:

- Автоматический;
- Ручной.

### 3.12.1 Автоматическое резервное копирование

Режим автоматического резервного копирования обеспечивает формирование файл-конфигурации узла фильтрации без участия администратора системы с заданной периодичностью и его размещение на корпоративном сетевом хранилище. Параметры настройки данного механизма представлены в модуле «Автоматический бэкап» (Рисунок 80).

Для корректировки настроек необходимо нажать на пиктограмму ✎ и указать следующие параметры:

- День бэкапа – в какие дни недели, необходимо производить формирование файла-конфигурации;
- Время бэкапа;
- Протокол – указать протокол, по которому будет производиться обращение к сетевому хранилищу для размещения файла-конфигурации;
- Хост\Имя компьютера или IP – FQDN имя или IP адрес сетевого хранилища;

- Раздел\Ссылка – указать раздел на сетевом хранилище, в который будет осуществляться размещение файла-конфигурации;
- Префикс бэкапа – имя создаваемого файла-конфигурации;
- Логин – имя учетной записи, при помощи которой будет осуществляться подключение к сетевому хранилищу;
- Password – пароль для вышеуказанной учетной записи.

По окончанию ввода параметров необходимо нажать кнопку «Сохранить».

Активация функционала автоматического резервного копирования осуществляется путем нажатия пиктограммы напротив поля «Включить бэкап».

Системой предусмотрен механизм принудительного запуска механизма автоматического резервного копирования (например, с целью проверки корректности настроек), для этого необходимо нажать кнопку «Создать бэкап», после чего будет сформирован файл-конфигурации и произойдет его размещение на сетевом хранилище в соответствии с вышеуказанными настройками.

Восстановление параметров узла фильтрации из файла-конфигурации осуществляется в модуле «Ручное управление бэкапом» (см. п.3.12.3).

### 3.12.2 Ручное управление резервным копированием

Механизм ручного резервного копирования позволяет создавать файл-конфигурацию параметров системы в ручном режиме и обеспечить его загрузку на рабочую станцию администратора. Для перехода в интерфейс ручного резервного копирования необходимо перейти в модуль «Ручной бэкап» (Рисунок 81).

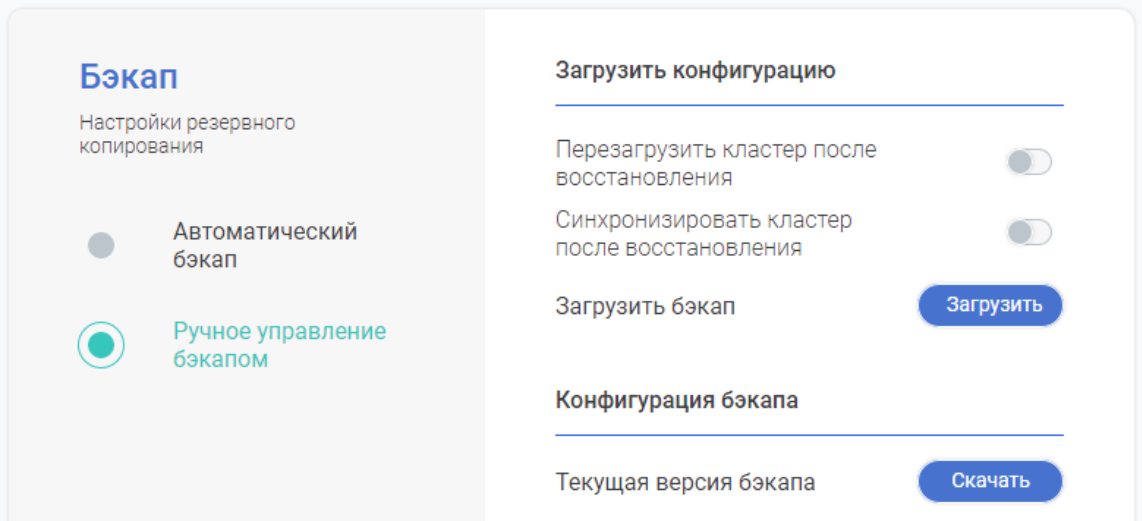


Рисунок 81 – Интерфейс ручного резервного копирования

Для создания файла-конфигурации и его загрузки на рабочую станцию администратора необходимо нажать кнопку «Скачать» в области «Конфигурация бэкапа», после чего произойдет его загрузка.

### 3.12.3 Восстановление из резервной копии

Восстановление параметров узла фильтрации из файла-конфигурации осуществляется в модуле «Ручное управление бэкапом» (Рисунок 81). Для выполнения данной процедуры

необходим в области «Загрузить конфигурацию» нажать кнопку «Загрузить», после чего выбрать файл-конфигурацию из которого необходимо произвести восстановление параметров узла фильтрации.

В случае, когда используется несколько узлов фильтрации объединенных в кластер конфигурации, существуют следующие рекомендации по восстановлению параметров:

- Если осуществляется добавление нового вспомогательного узла фильтрации в кластер конфигурации, то возможно использовать файл-конфигурацию на этапе первичной настройки узла фильтрации и добавления его в кластер;
- Если осуществляется восстановления основного узла фильтрации в кластере конфигурации, то при процедуре восстановления возможно указать параметры автоматической перезагрузки и синхронизации кластера с целью применения настроек фильтрации на всех узлах кластера из восстанавливаемого файла-конфигурации основного узла.

## 3.13 Статистика и логирование

### 3.13.1 Статистика обработки пользовательских запросов

Работа с инструментам по предоставлению статистической информации осуществляется в разделе «Статистика и логирование» в меню «Kibana» (Рисунок 82).

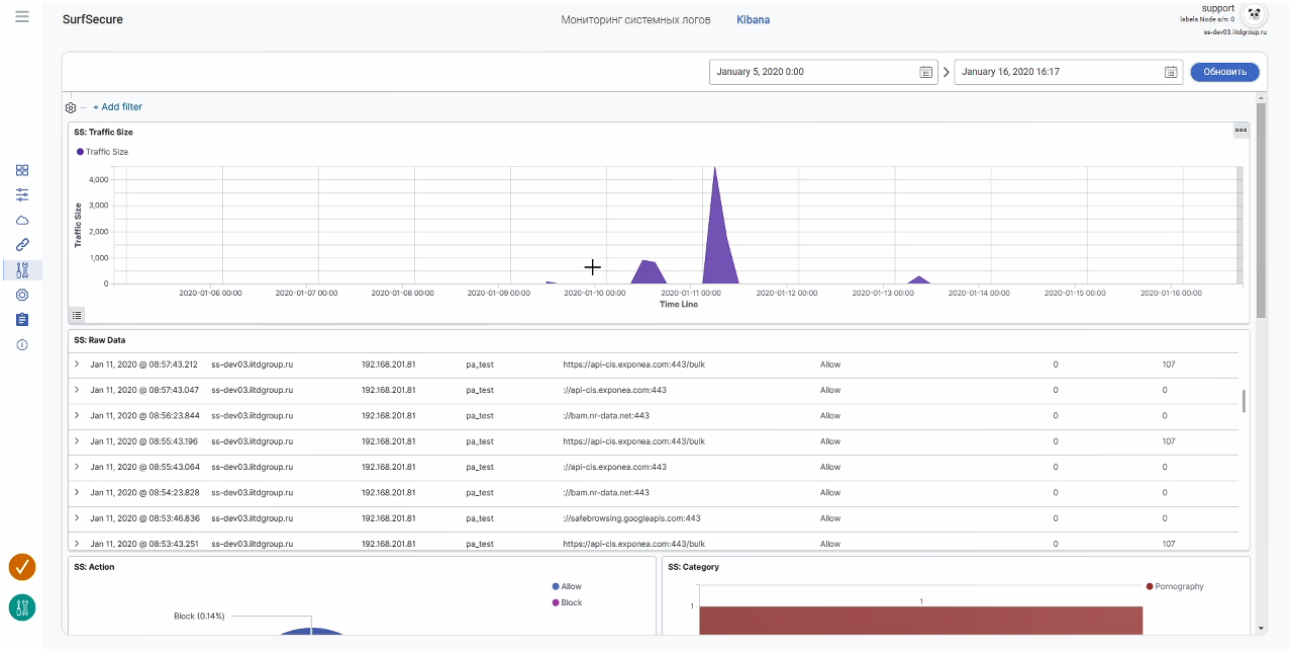


Рисунок 82 – Интерфейс работы со статистической информацией

Данный интерфейс показывает статистику работы внутренних механизмов фильтрации и детальную информацию по запросам за выбранный временной промежуток. Для формирования выборки статистической информации необходимо указать интересующий временной интервал 

и нажать кнопку «Обновить». При необходимости, существует возможность добавления дополнительных фильтров, для этого необходимо нажать кнопку «Add filter» и выбрать

необходимый параметр. Далее интерфейс отобразит статистическую информацию по обработанному трафику пользователей в виде графиков и справочной информации в следующих окнах:

- SS:Traffic Size – объем обработанного трафика в зависимости от времени выбранного интервала;
- SS:RAW Data – информация по запросам пользователей:
  - Time – время обработки запроса;
  - Hostname – узел фильтрации, обработавший запрос;
  - IP – IP адрес пользователя;
  - Login – имя учетной записи пользователя;
  - URL – запрошенный веб ресурс;
  - Policy_type - отображает механизм для правила которое совпало;
  - Action – результат обработки запроса;
  - Cat_name – принадлежность запрошенного веб ресурса к предустановленным категориям;
  - Rule_id – уникальный идентификатор правила фильтрации, под который попал данный запрос;
  - Size – размер запроса.
- SS:Action – сводная информация по соотношению разрешенных и заблокированных запросов;
- SS:Category – перечень категорий веб ресурсов с количество вхождений по запросам пользователей;
- SS:Top Users – перечень учетных записей пользователей с указанием процентного соотношения объема обработанного трафика;
- SS:Top IP – перечень IP адресов с указанием процентного соотношения объема обработанного трафика;
- SS:Engine – перечень механизмов фильтрации с указанием процентного соотношения объема срабатывания;
- SS:AV Table – перечень типов вредоносного ПО с указанием процентного соотношения объема попыток загрузки файлов.

### 3.13.2 Системные логи

Системные логи включают в себя всю информацию о работе всех системных компонент узла фильтрации. Интерфейс работы с системными логами расположен в разделе «Статистика и логирование» в меню «Мониторинг системных логов» (Рисунок 83).

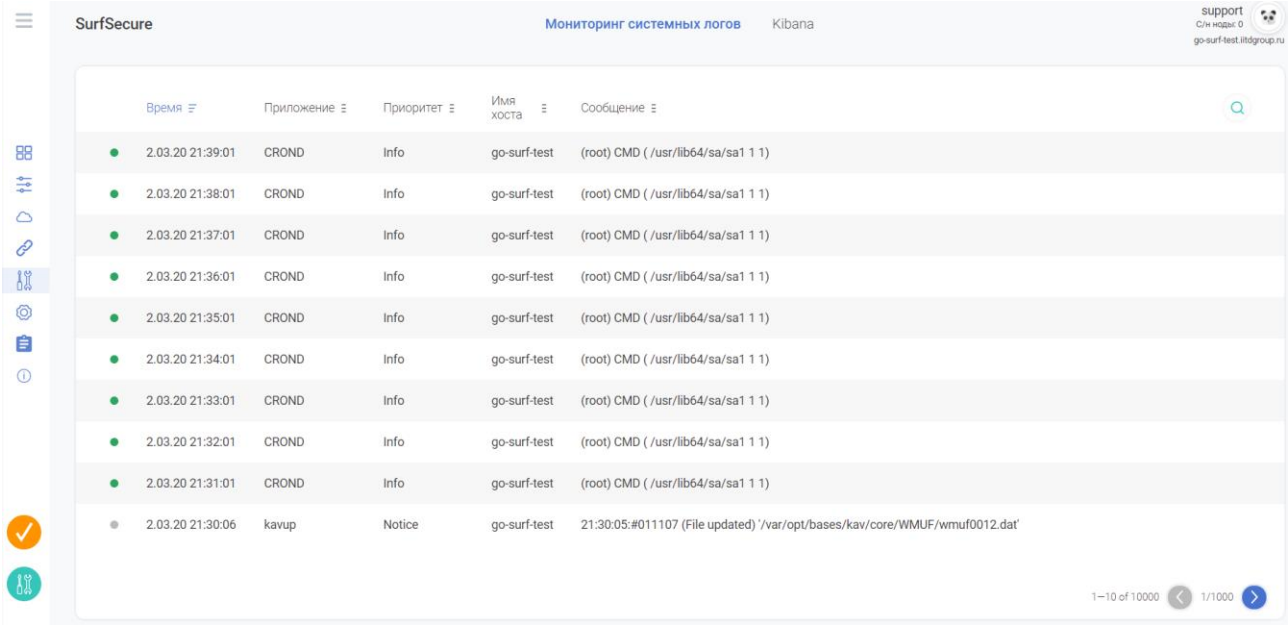


Рисунок 83 – Интерфейс просмотра системных логов

Данный интерфейс по умолчанию отображает всю информацию по работе внутренних служб в хронологическом порядке, отображая самые новые сообщения в начале. Интерфейс отображает на странице не более 10 сообщений, для навигации между страницами необходимо воспользоваться курсором 1/1000 в правой нижней части экрана. Существует возможность сортировки информации по выбранному параметру, для этого необходимо нажать пиктограмму рядом с выбранными параметром.

В левой части каждого сообщения отображена цветовая индикация важности данного события:

- Серый – уведомление (Notice\Debug);
- Зеленый – информационное (Info);
- Желтый – предупреждение (Warning);
- Красный – ошибка (Error\Alert).

Вся информация о событии отображается в соответствующей строке, при нажатии на строку записи будет отображено отдельное всплывающее окно с отображением информации по данному сообщению(Рисунок 84).

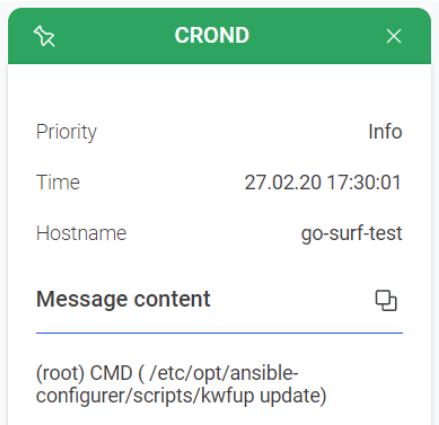


Рисунок 84 – Детальная информация о системном сообщении

Для копирования содержания данного сообщения в буфер обмена необходимо нажать на пиктограмму .

Интерфейс системы предусматривает два инструмента для поиска:

- Быстрый поиск;
- Расширенный поиск.

Быстрый поиск предназначен для упрощенного поиска и вывода информационных сообщений, которые соответствуют поисковому запросу. Для этого необходимо нажать пиктограмму и ввести поисковый запрос в появившуюся строку запроса.

Расширенный поиск предназначен для поиска системных сообщений по определенным параметрам и критериям. Для отображения интерфейса расширенного поиска необходимо также нажать пиктограмму и далее выбрать иконку , после чего отобразится дополнительное окно для ввода параметров поиска (Рисунок 85).

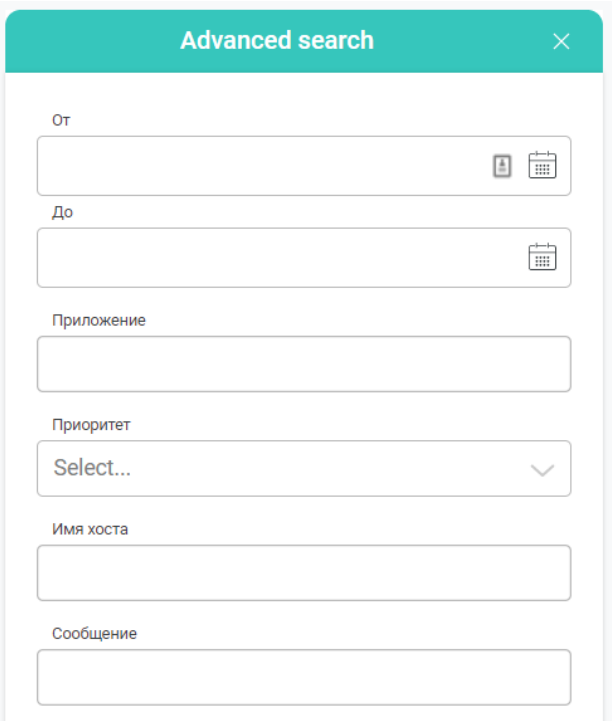


Рисунок 85 – Окно расширенного поиска

Существуют следующие возможности по указанию дополнительных фильтров:

- «От» и «До» - указание временного интервала для поиска;
- Приложение – поиск сообщений от выбранного приложения;
- Приоритет – уровень важности события;
- Имя хоста – выбор узла фильтрации, где было зарегистрировано сообщение;
- Сообщение – поисковый запрос по тексту системного сообщения.

Для расширенного поиска необходимо указать один или несколько вышеуказанных параметров и нажать кнопку «Искать», после чего на основном экране интерфейса будет отображен перечень всех системных сообщений, попадающих по заданный фильтр.

## 3.14 Лицензионная информация

Для того, чтобы просмотреть информацию о текущей лицензии или активировать новую лицензию необходимо перейти в раздел «Базовые настройки» в меню «Лицензия», после чего отобразится интерфейс работы с лицензионной информацией (Рисунок 86).

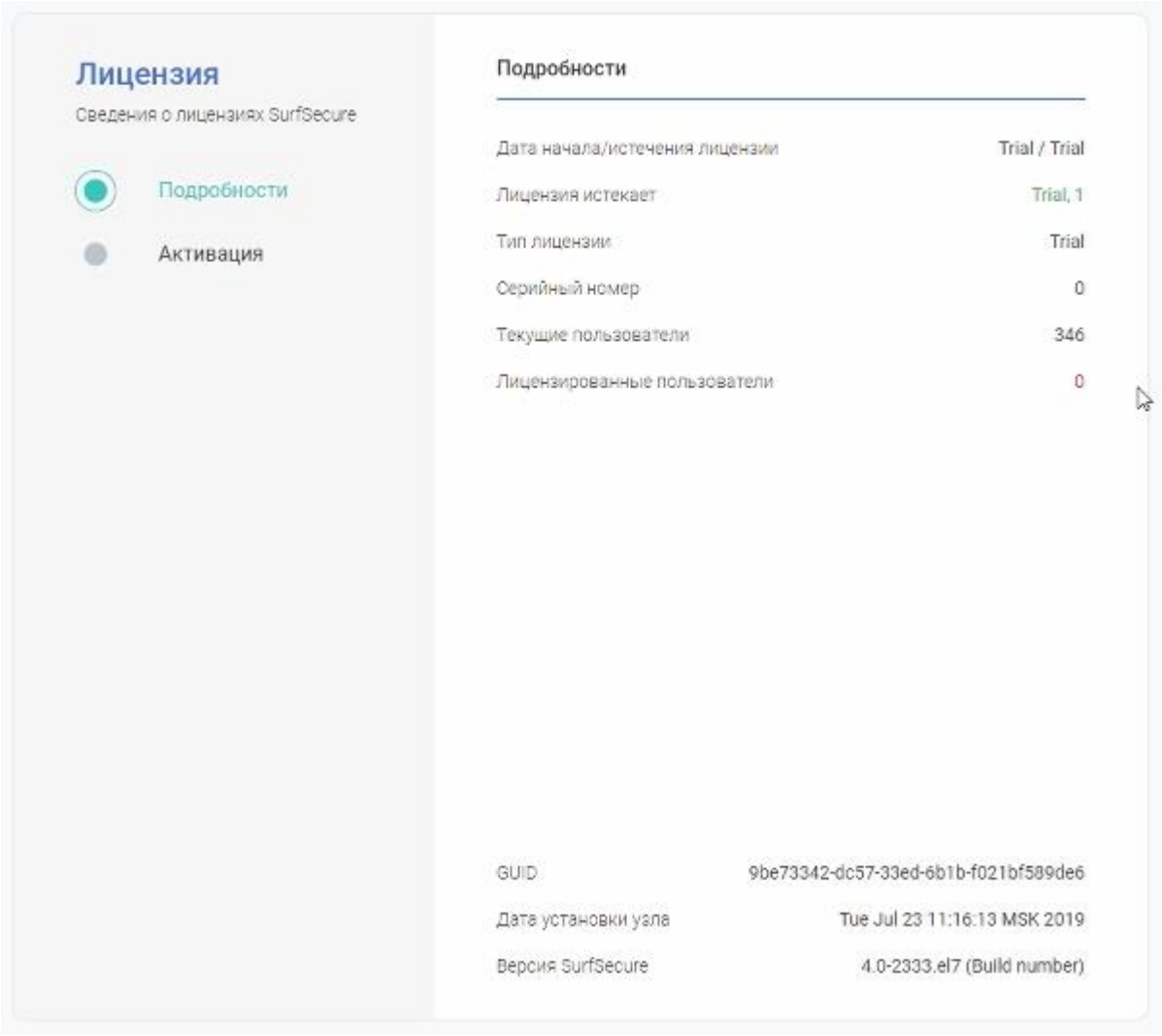


Рисунок 86 – Интерфейс просмотра параметров установленной лицензии

Меню работы с лицензионной информации содержит в себе два модуля:

- Подробности – информация о текущей лицензии;
- Активация – интерфейс для активации новой лицензии.

Для просмотра информации о текущей лицензии необходимо выбрать модуль «Подробности». В данном разделе представлена следующая информация:

- Дата начала\истечения лицензии – даты начала и окончания действия текущей лицензии;
- Лицензия истекает – количество дней до истечении лицензии;
- Тип лицензии – указывается тип лицензии (временная или постоянная);
- Серийный номер – уникальный идентификатор лицензии;
- Текущие пользователи – количество пользователей, чьи запросы система обрабатывает в настоящий момент времени;
- Лицензированные пользователи – количество пользователей, для которых действует текущая лицензия.

В случае, если количество текущих пользователей превышает количество лицензированных пользователей, то Система осуществит импорт из LDAP каталога количество пользователей, которое позволяет лицензия.

В нижней части страницы приведена дополнительная справочная информация:

- GUID – уникальный идентификатор узла фильтрации;
- Дата установки узла – дата инсталляции и первого запуска узла фильтрации;
- Версия SurfSecure – текущая версия ПО.

Установка нового лицензионного ключа для работы системы осуществляется в меню «Активация» (Рисунок 87).

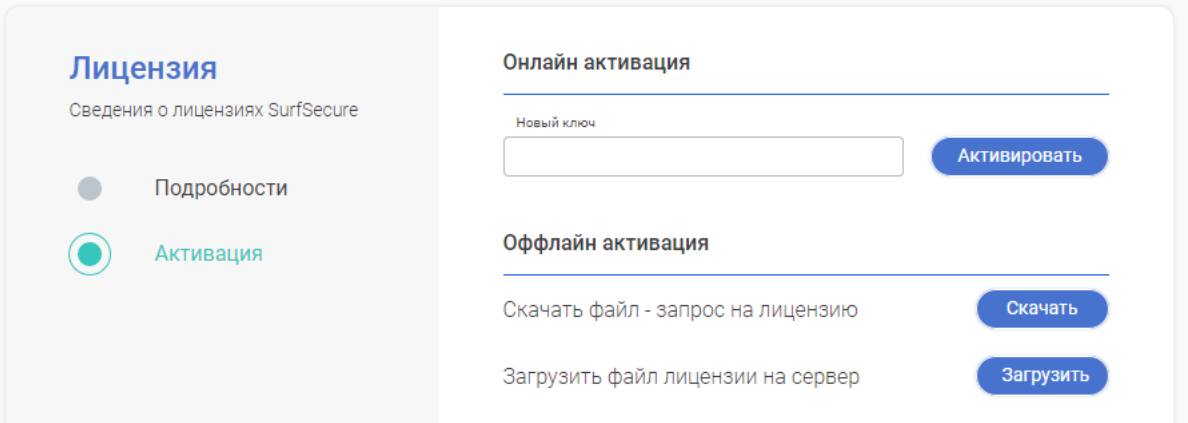


Рисунок 87 – Интерфейс меню активации лицензионного ключа

В системе предусмотрено два способа установки и активации лицензионного ключа:

- Онлайн активация;
- Оффлайн активация.

Способ онлайн активации является наиболее предпочтительным и может быть использован, если у системы есть доступ в сеть интернет. Для этого в поле «Новый ключ» необходимо ввести уникальный ключ в формате XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX и нажать кнопку «Активировать». По окончанию операции будет отображено всплывающее окно с информацией об успешности выполнения данной операции.

В случае отсутствия у системы подключения к сети интернет необходимо воспользоваться методом «Оффлайн активации». Для этого необходимо выполнить следующую последовательность действий:

1. Нажать кнопку «Скачать», после чего осуществится загрузка файла—запроса на рабочую станцию администратора;
2. Передать данный файл-запрос в сторону производителя;
3. Получить от производителя лицензионный файл и осуществить его установку с использованием кнопки «Загрузить».

По окончанию операции будет отображено всплывающее окно с информацией об успешности выполнения данной операции.

## 3.15 Диагностика и отладка

Система предусматривает набор инструментов администратора для отладки работы системы и проверки наличия доступа к тем или иным ресурсам. Для доступу к интерфейсу инструментов необходимо перейти в раздел «Базовые настройки» в меню «Инструменты» (Рисунок 88).

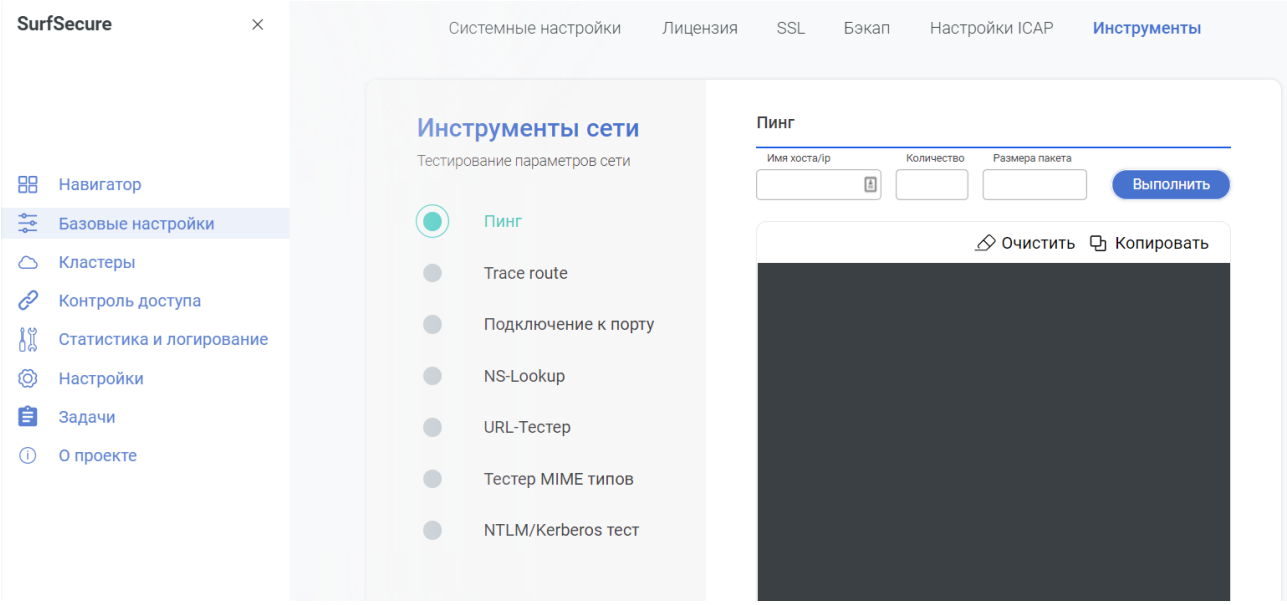


Рисунок 88 – Интерфейс работы с инструментами отладки

Набор инструментов для отладки включает в себя следующие модули:

- Пинг – проверка доступности сетевого ресурса по протоколу ICMP. Указывается:
  - Имя хоста\IP – IP адрес или FQDN имя сервера до которого требуется проверить доступность;
  - Количество (опционально) – количество пакетов для отправки. Пустое поле означает непрерывный режим;
  - Размер пакет (опционально) – размер пакета для отправки.
- Trace route – отслеживание маршрута прохождения сетевого пакета. Указывается:
  - Имя хоста\IP – IP адрес или FQDN имя сервера до которого требуется отследить маршрут.
  - Resolution – необходимость разрешения имени промежуточного хоста;
- Подключение к порту – проверка возможности подключения по TCP порту или отправка UDP пакета. Указывается:
  - Имя хоста\IP – IP адрес или FQDN имя сервера до которого требуется проверить доступность;
  - Порт – порт, к которому требуется осуществить подключение;
  - Протокол – TCP или UDP.
- NS-Lookup – проверка корректности работы механизма DNS и запрос различных типов записей для доменных имен. Указывается:

    - Имя хоста\I – IP адрес или FQDN для которого необходимо сделать запрос в DNS;
    - Хост\IP сервера (опционально) – IP адрес DNS сервера для запроса параметров. Пустое поле означает использование DNS сервера в соответствии с настройками узла фильтрации;
    - Тип – выбор типа записи для запроса.
- URL-Тестер – проверка принадлежности веб ресурса к определённой категории. Указывается:
    - URL – адрес веб ресурса для определения категории.
    - Расширенный вывод – отображения дополнительной диагностической информации.
- Тестер MIME типов – проверка принадлежности файлов к определенному MIME типу, а также просмотр временных задержек при доступе к веб ресурсу. Указывается:
    - URL – адрес веб ресурса или прямая ссылка на файл.
- NTLM\Kerberos тест – проверка доступности внешних сервисов для авторизации, если такая интеграция была ранее настоена.

Для всех инструментов существует возможность копирования текста вывода в буфер обмена путем нажатия кнопки «Копировать». Для того, чтобы очистить содержимое поля вывода необходимо нажать кнопку «Очистить».

# 4 Источники разработки

Настоящее Техническое задание разработано на основе следующих информационных материалов и документов:

– ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения;

– ГОСТ 34.601-90 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;

– ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;

– ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;

– ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем;

– РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов;

– РД 50-680-88 Методические указания. Автоматизированные системы. Основные положения.

# Приложение 1 – Рекомендации по выпуску сертификата

Созданный файл запрос (CSR-файл) необходимо использовать для выпуска сертификата через корпоративный центр сертификации. Для этого необходимо войти в интерфейс центра сертификации через:

- Веб интерфейс;
- Оснастку MMC.

Далее необходимо подписать запрос, для этого необходимо выбрать пункт Request certificate-> Advanced Certificate request. В зависимости от используемого интерфейса необходимо либо импортировать CSR файл (оснастка MMC), либо вставить содержимое файла (веб интерфейс) в поле Saved Request. В шаблоне выпуска сертификата необходимо выбрать предустановленный шаблон Subordinate authority (или «Подчиненный центр сертификации»), в поле Additional attributes добавить атрибут Subject Alternative Name в формате «san:dns=node1.domain.com&dns=node1».

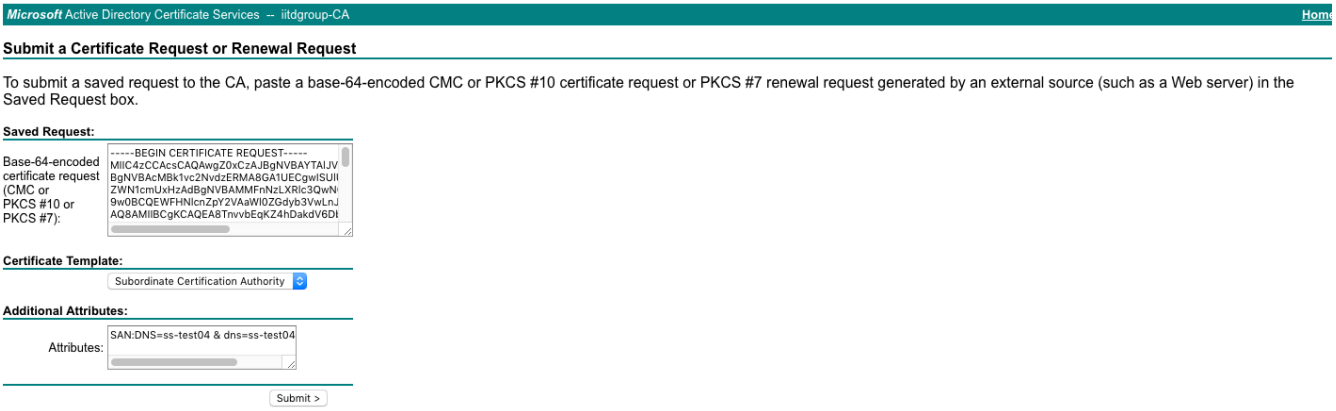


Рисунок 89 – Подписание запроса на выпуск сертификата

Следующим шагом необходимо отправить запрос и скачать сертификат в формате base64 и произвести его установку на узел фильтрации.

### Замечание:

В настройках центра сертификации должна быть активирована и разрешена вставка дополнительных атрибутов в сертификат.