AVSOFT KAIROS v2

Система защиты от спама и фишинга

Руководство администратора

Москва
2024

Контактная информация

127106, г. Москва, ул. Гостиничная, д.5

Тел.: +7 (495) 988-92-25

E-mail: office@avsw.ru

www.avsw.ru/about/contacts

Авторское право

Версия документа

Руководство администратора v2.4

Апрель 5, 2024.

СОДЕРЖАНИЕ

1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице 1.

Таблица 1. Термины и определения

№	Термин	Определение
1.	Эксплайнер	Короткий видеоролик, который используется для объяснения сложных и абстрактных функций и действий.
2.	API	«Программный интерфейс приложения» — описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой.
3.	DKIM	Метод аутентификации отправителя письма при помощи создания цифровой подписи доменных ключей и ее проверки получателем.
4.	DMARC	Политика проверки подлинности отправителя письма с использованием механизмов DKIM и SPF.
5.	DNS	Компьютерная распределенная система для получения информации о доменах.
6.	ID	Уникальный идентификатор.
7.	ML	Модели машинного обучения анализируют письма на принадлежность к спаму и ссылки - на принадлежность к фишингу.
8.	SPF	Метод, используемый для верификации серверов в домене отправителя, с помощью их перечисления в txt-записи DNS-запроса.
9.	Spam Score	Набор правил для фильтрации спама, которые анализируют текст и заголовок письма. В правилах также используются методы DKIM и Spam Score.

№	Термин	Определение
10.	Soft Fail	Подход для обработки ошибки в приложении. Soft Fail немедленно прекращает работу и сообщает об ошибке.
11.	Perm Error	Указывает, что во время проверки сообщения произошла постоянная ошибка DNS сервера.
12.	Temp Error	Указывает, что во время проверки сообщения произошла временная ошибка DNS сервера.

2 Перечень сокращений

В настоящем документе используется перечень сокращений, представленный в таблице 2.

Таблица 2. Перечень сокращений

№	Сокращение	Значение
1.	AD	Active Directory
2.	AES	Advanced Encryption Standard
3.	API	Application Programming Interface
4.	CPU	Central Processing Unit
5.	DKIM	Domain Keys Identified Mail
6.	DMARC	Domain-based Message Authentication, Reporting and Conformance
7.	DNS	Domain Name System
8.	ID	Identifier
9.	ML	Machine Learning
10.	SIEM	Security information and event management
11.	SHA	Secure Hash Algorithm
12.	SPF	Sender Policy Framework

3 Введение

Система защиты от спама и фишинга AVSOFT KAIROS v2 (далее – Система) предназначена для комплексного обнаружения и фильтрации спама, а также фишингового контента в реальном времени.

Система способна анализировать данные из следующих источников:

- Почтовый трафик
- Мессенджеры
- API

Система осуществляет следующие виды проверок и анализа:

- Проверка на спам
- Проверка фишинг
- Проверка на вредоносные вложения

3.1 Режимы работы

Проверку почтового трафика Система поддерживает в режимах, описанных в таблице 3.

Таблица 3. Описание режимов проверки

№	Режим	Описание режима
1.	«Зеркало»	Пользователь получает письмо и одновременно с этим происходит проверка его вложений в системе на наличие вредоносных элементов.
2.	«В разрыв»	Сначала идет проверка вложений письма в системе, а потом пользователь их получает, если им присвоен безопасный вердикт.

3.2 Поддержка Системы

Система поддерживает расшифрование входящего почтового трафика (SMTP over TLS).

Система поддерживает возможность блокировки сессии, если отправитель попытается передать сообщение без шифрования.

Система поддерживает возможность настройки группы отправителей, которые могут работать только по SMTP over TLS.

Система не имеет ограничений. Необходимая производительность Системы достигается за счет увеличения количества компонентов.

Система имеет возможность горизонтального масштабирования без изменения архитектуры.

3.3 Внешние ресурсы

Список внешних ресурсов, к которым идет обращение Системы в процессе анализа, представлен в таблице 4.

Таблица 4. Внешние ресурсы

№	Название	Ресурс	Описание
1.	Проверка домена	XSEO	http://xseo.in
2.		UrlScan	https://urlscan.io
3.		PhishTank	http://phishtank.org
4.	Проверка ссылки и домена	VirusTotal	https://www.virustotal.com/
5.	Позиция в рейтинге Alexa Rank	Alexa Rank	http://data.alexa.com/
6.	Индексация в Google	Google	http://google.com
7.	Наличие в Интернет-архиве	Wayback Machine - Internet Archive	http://web.archive.org
8.	Информация о домене	WHOIS	https://www.whois.com
9.	Боты вредоносных ссылок	OpenFish	https://openphish.com/
10.		PhishTank	http://data.phishtank.com
11.		GitHub	https://raw.githubusercontent.com

№	Название	Ресурс	Описание
12.	Прослушка каналов с фишингом и парсинг ссылок	Телеграмм бот	https://telegram.org/

При локальной работе системы без Интернета идет обращение к локальной БД следующих ресурсов:

- рейтинг Alexa
- рейтинг Pagerank
- БД вредоносных хэшей

4 Требования

4.1 Персонал и квалификация

Общие требования к специалистам, осуществляющим администрирование Системы:

- опыт в администрировании систем Debian
- опыт в администрировании СУБД (PostgreSQL, MongoDB)
- знание основ сетевого администрирования
- знание технологий контейнеризации (Docker)
- опыт в администрировании SIEM
- опыт в администрировании почтовых серверов (SMTP)
- знание основ резервного копирования

4.2 Инфраструктурные компоненты

Основные инфраструктурные модули, используемые в Системе, представлены в следующем списке:

- Debian
- Docker
- Flask
- MongoDB
- PostgreSQL

– Python

– RabbitMQ

5 Активация и настройки

В разделе «Настройки» осуществляется настройка всех модулей Системы.

5.1 Общие настройки

После установки Системы на сервер администратору производителем выдается логин, пароль и файл-ключ активации лицензии. Необходимо выполнить авторизацию в графическом интерфейсе и активировать лицензию.

Для активации лицензии на использование Системы необходимо перейти в раздел «Настройки» → «Основные» → «Лицензия» (Рисунок 1).

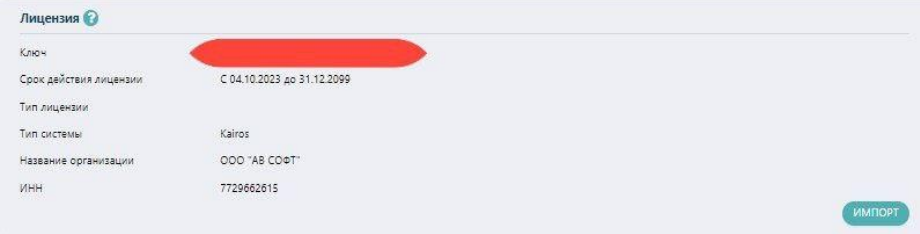

Рисунок 1. Раздел «Настройки»

Далее необходимо загрузить в систему выданный производителем файл-ключ с помощью кнопки «Импорт», после нажатия на которую отобразится форма «Импорт лицензии» (Рисунок 2).

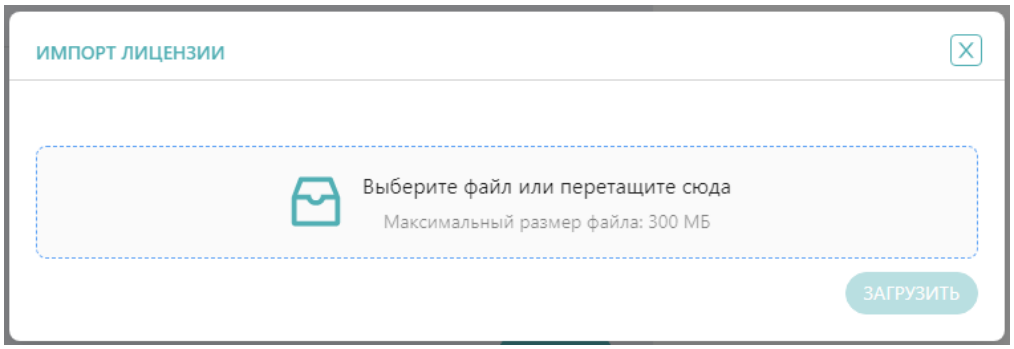

Рисунок 2. Форма «Импорт лицензии»

После загрузки файла-ключа автоматически заполнятся следующие поля в функциональном блоке:

– Срок действия лицензии

– Тип лицензии

– Тип системы

– Название организации

– ИНН организации

Если действие выполнено успешно, то отобразится сообщение «Настройки сохранены».

Во вкладке «Настройки» - «Основные» - «Системные» есть возможность выбора режима системы (Полный или быстрый) (Рисунок 3)

Полный режим включает в себя все виды анализа ссылок (история переходов, информация по домену, анализ с помощью машинного обучения, визуальный анализ и скриншоты, анализ заголовков), что требует от системы ресурсов больше, чем в быстром режиме.

Быстрый режим исключает анализ скриншотов, получение информации по домену и использование моделей с большим весом и эксплайнеров для машинного обучения при исследовании ссылки.

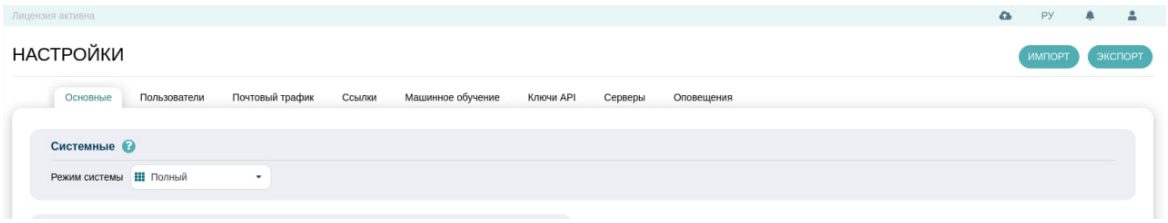

Рисунок 3. Выбор режима Системы

Также в данном разделе реализована возможность импорта и экспорта настроек системы из файла и в файл соответственно.

Для экспортирования настроек предназначена кнопка «Экспорт», расположенная в правой верхней части экрана, после нажатия на которую автоматически начнется выгрузка файла с сохраненными настройками системы. Пример выгрузки файла с сохраненными настройками представлен ниже (Рисунок 4).

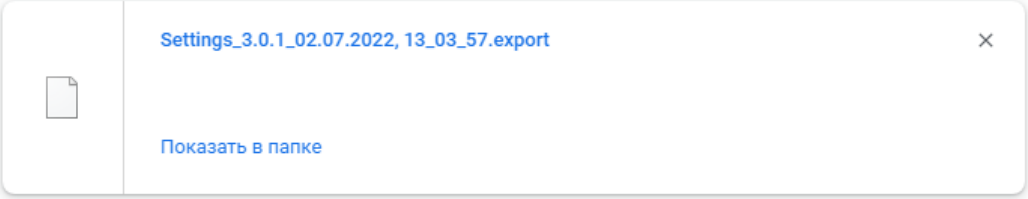

Рисунок 4. Загрузка файла с сохраненными настройками

Для импортирования настроек будет использоваться, соответственно, кнопка «Импорт», расположенная так же в правой верхней части экрана. Далее появится окно, где необходимо выбрать/перетащить файл, содержащий сохраненные настройки системы (Рисунок 5).

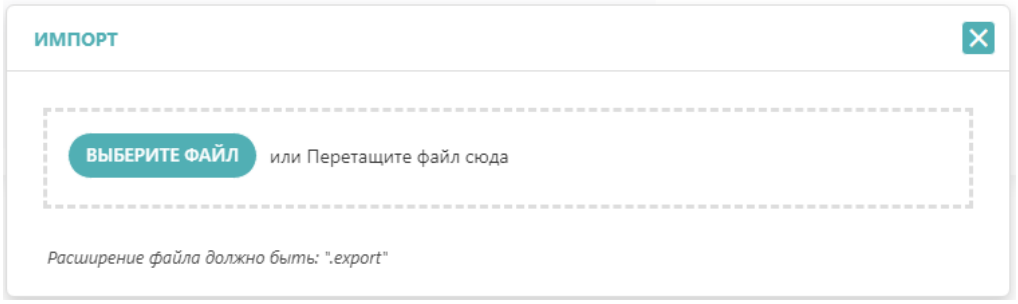

Рисунок 5. Окно импорта настроек

После этого в нижней части экрана отобразится уведомление об успешном применении сохраненных настроек (Рисунок 6).

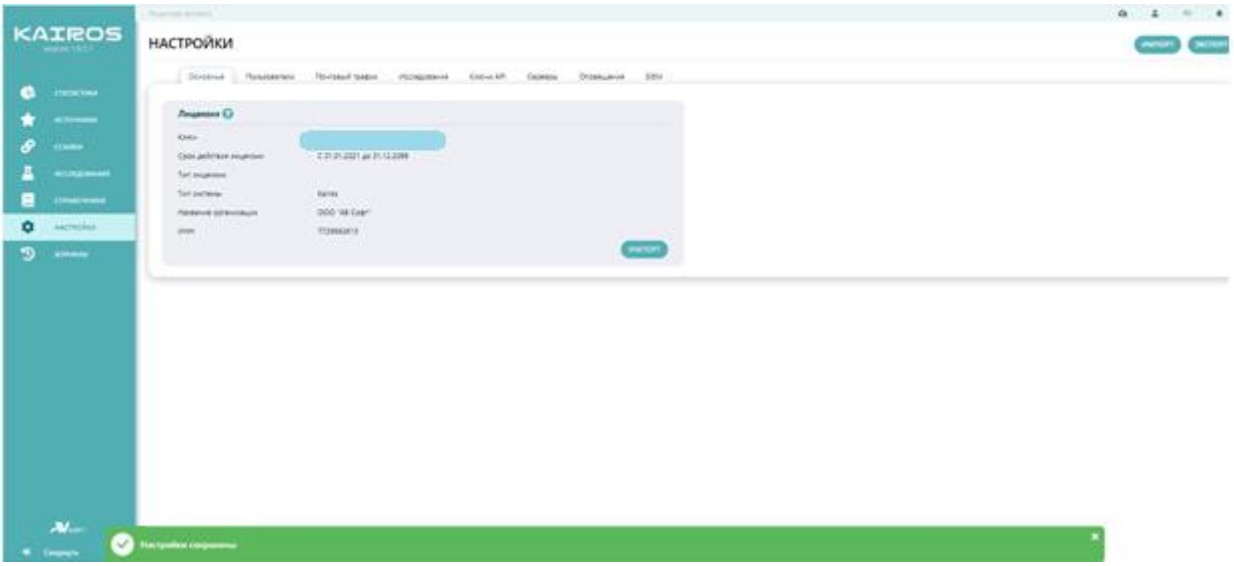

Рисунок 6. Уведомление об успешном применении сохраненных настроек

5.2 Управление пользователями Системы

В Системе управление пользователями осуществляется во вкладке «Пользователи» (Рисунок 7).

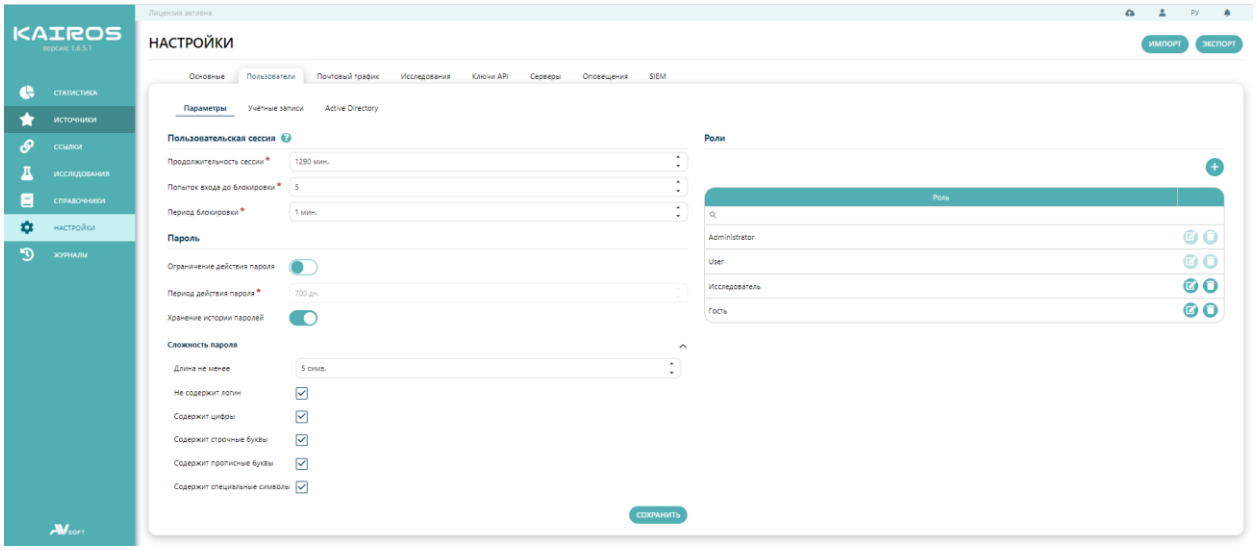

Рисунок 7. Раздел «Настройки», вкладка «Пользователи»

Во вкладке «Параметры» в функциональном разделе «Пользовательская сессия» присутствуют параметры настройки пользовательской сессии, при превышении которых произойдет блокировка текущей сессии пользователя в Системе. Описание параметров приведено в таблице 5.

Таблица 5. Описание параметров «Пользовательская сессия»

№	Параметры	Описание
1.	Продолжительность сессии	Период времени (в минутах), по истечении которого, в случае бездействия пользователя, произойдет блокировка текущей сессии.
2.	Попытки входа до блокировки	Количество неудачных попыток входа, после которых произойдет блокировка.
3.	Период блокировки	Время, на которое пользователь будет заблокирован

В разделах «Пароль» и «Сложность пароля» находятся настройки правил и требований при создании пароля для входа в Систему. В таблице 6 описаны параметры настроек.

Таблица 6. Описание параметров настройки пароля

№	Параметры	Описание
1.	Ограничение действия пароля	Флаг, который активирует режим ограничения пароля в системе.
2.	Период действия пароля (дни)	Устанавливается период времени, по истечении которого пароль должен быть сменен.
3.	Хранение истории паролей	Флаг, который активирует возможность системе по каждому пользователю сохранять историю паролей.

В функциональном разделе «Роли» отображается список ролей в системе по умолчанию. Для добавления новой роли с определенным набором прав необходимо нажать кнопку «Добавить», которая отобразит функциональную форму «Настройки роли» (Рисунок 8).

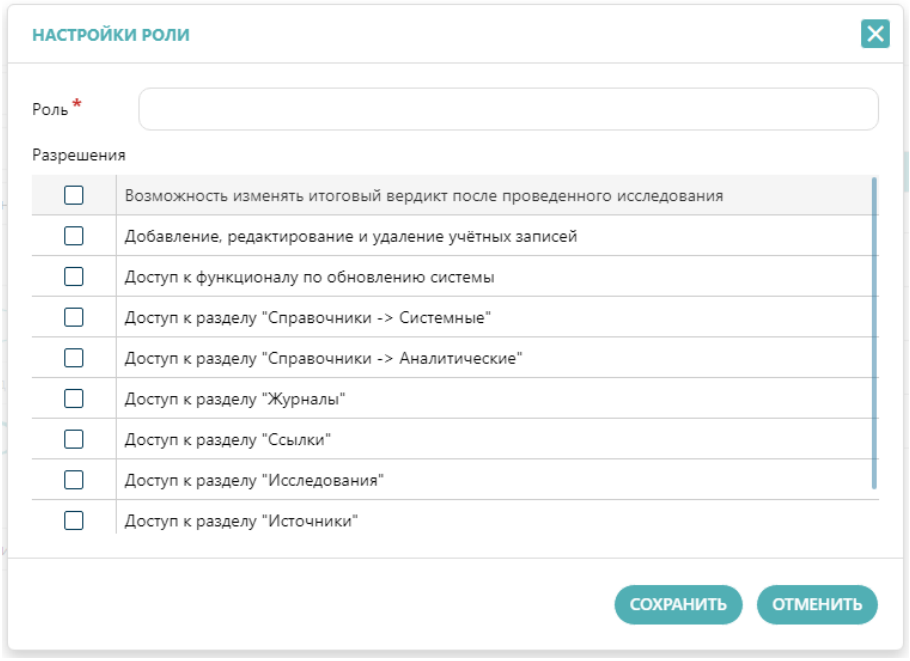

Рисунок 8. Добавление новой роли

В отобразившейся форме необходимо указать параметры, описанные в таблице 7.

Таблица 7. Описание параметров для создания новой роли

№	Параметры	Описание
1.	Роль	Название новой роли, создаваемой в системе.
2.	Разрешения	
2.1	Общая возможность добавления, редактирования и удаления	Добавление прав на общие возможности добавления, редактирования и удаления.
2.2	Скачивание файлов из системы	Добавление прав на скачивание файлов из системы
2.3	Доступ к функционалу по обновлению системы	Добавление прав на обновление системы.
2.4	Доступ к разделу «Политики»	Добавление прав доступа к разделу «Политики»

№	Параметры	Описание
2.5	Доступ к разделу «Справочники → Системные»	Добавление прав доступа к разделу «Справочники» → «Системные».
2.6	Доступ к разделу «Справочники → Аналитические»	Добавление прав доступа к разделу «Справочники» → «Аналитические».
2.7	Доступ к разделу «Журналы»	Добавление прав доступа к разделу «Журналы».
2.8	Доступ к разделу «Политики»	Добавление прав доступа к разделу «Политики».
2.9	Доступ к разделу «Ссылки»	Добавление прав доступа к разделу «Ссылки».
2.10	SourcesAccess	Добавление прав доступа к разделу «SourcesAccess».
2.11	Доступ к разделу «Почтовый трафик»	Добавление прав доступа к разделу «Почтовый трафик».
2.12	Доступ к разделу «Спутники»	Добавление прав доступа к разделу «Спутники».
2.13	Доступ к разделу «Спутники» - «Агенты»	Добавление прав доступа к разделу «Спутники» - «Агенты»
2.14	Доступ к разделу «Ресурсы»	Добавление прав доступа к разделу «Ресурсы».
2.15	Возможность просматривать запись исследования в отчете по динамическому исследованию	Добавление прав на возможность просматривать записи исследований

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что созданная роль отобразилась в таблице всех ролей

системы. Имеется возможность редактирования доступа к разделам у готовых ролей.

Во вкладке «Учетные записи» присутствует информация по всем зарегистрированным пользователям в системе (Рисунок 9).

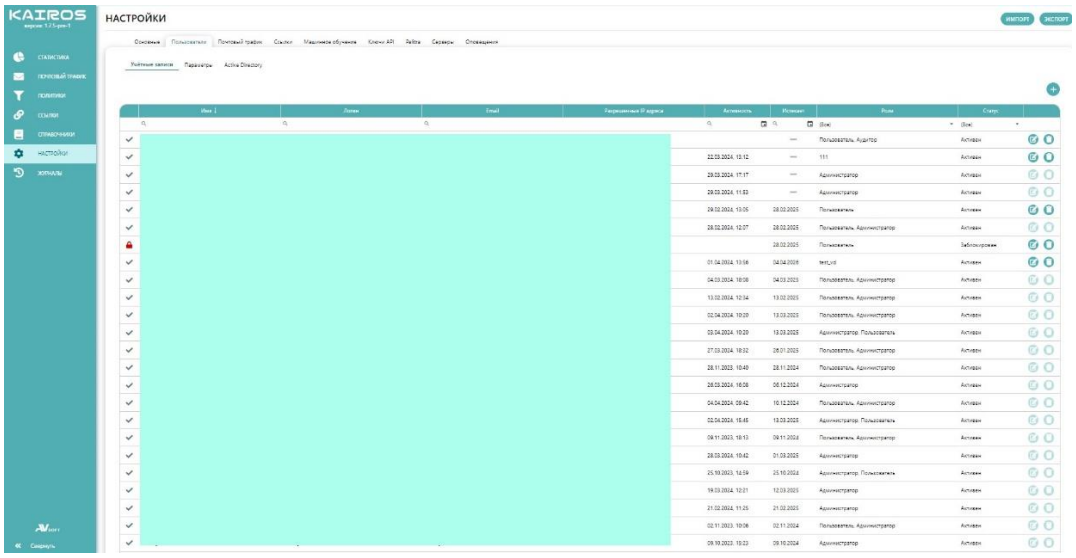

Рисунок 9. Зарегистрированные в системе пользователи

Пользователь с правами суперадмина может редактировать и удалять других пользователей, у которых есть права админа. При наличии у пользователя только прав админа, нельзя редактировать и удалять пользователей с такими же правами. Для добавления нового пользователя в Систему суперадмину необходимо нажать на кнопку с иконкой «Добавить», далее осуществится переход в форму для заполнения регистрационных данных о новом пользователе (Рисунок 10).

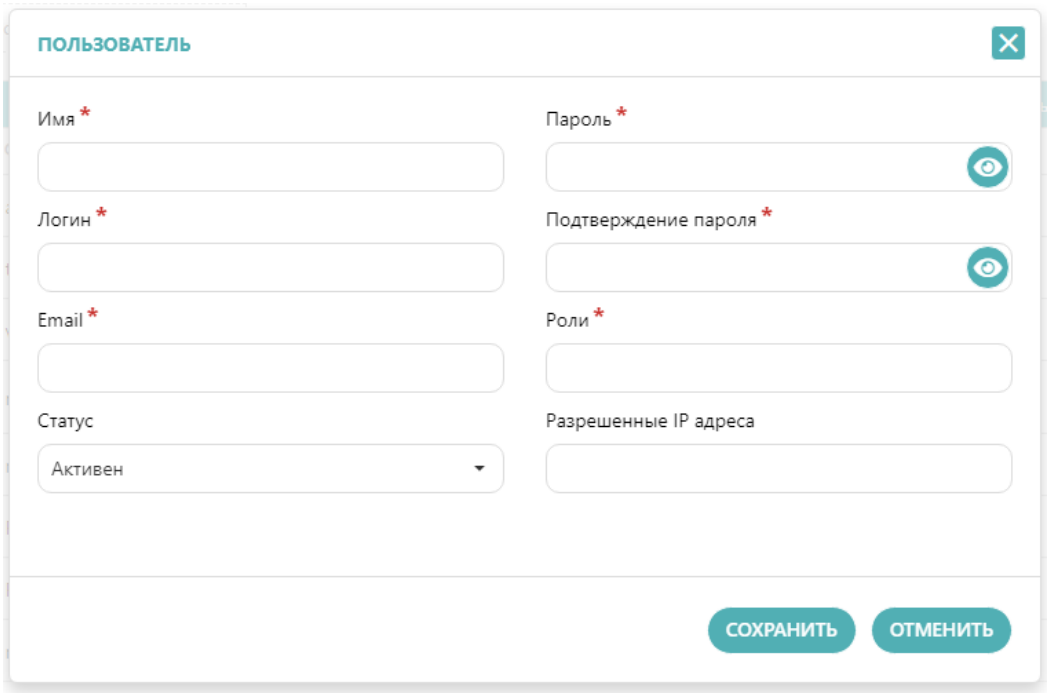

Рисунок 10. Добавление нового пользователя

Далее необходимо указать параметры, описанные в таблице 8.

Таблица 8. Описание параметров для создания нового пользователя

№	Параметры	Описание
1.	Имя	Имя пользователя в системе.
2.	Логин	Логин для авторизации в системе.
3.	Email	Электронная почта для подтверждения авторизации и восстановления пароля.
4.	Статус	Статус пользователя в системе, который имеет два состояния: – Заблокирован – Активен
5.	Пароль	Пароль для входа в систему.
6.	Подтверждение пароля	Подтверждение пароля для входа в систему.
7.	Роли	Пользовательские роли в системе с предустановленным набором прав:

№	Параметры	Описание
		– Пользователь (не имеет доступа к настройкам системы), – Администратор (имеет доступ ко всем разделам в системе).
8.	Разрешенные IP адреса	Перечисление IP-адресов разрешенные к использованию.

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новый созданный пользователь отобразился в общей таблице всех пользователей системы.

Для блокировки пользователя в системе необходимо нажать на иконку «Редактировать» в общей таблице пользователей. Далее в окне профиля пользователя «Пользователь» в поле «Статус» в выпадающем меню выбрать «Заблокирован», далее необходимо нажать кнопку «Сохранить» и удостовериться, что в общей таблице пользователей измененный статус пользователя отобразился корректно.

Во вкладке «Active Directory» отображается общая таблица доменов, где назначается адрес сервера, контролирующий область компьютерной сети, назначается домен и режим поиска уникальных имен (Рисунок 11).

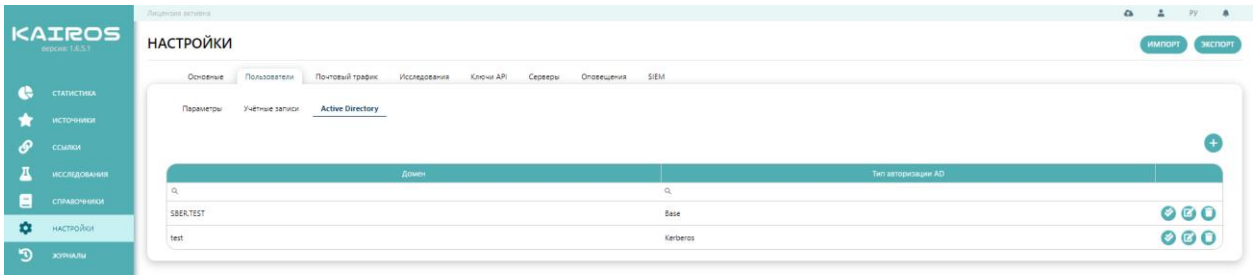

Рисунок 11. Вложенная вкладка «Active Directory»

Для добавления домена в таблицу «Active Directory», необходимо нажать кнопку «Добавить». Пример отображения формы добавления домена «Active Directory» представлен ниже (Рисунок 12).

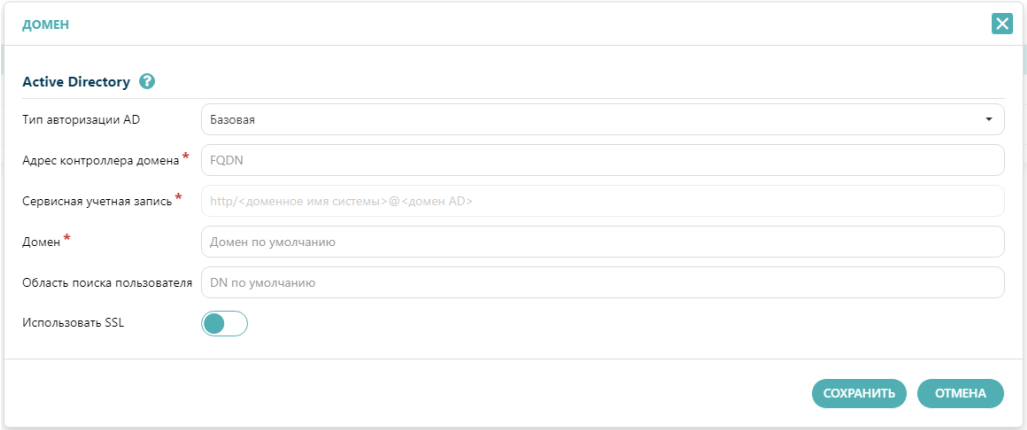

Рисунок 12. Форма «Домен Active Directory»

В отобразившейся форме необходимо указать параметры, описанные в таблице 9.

Таблица 9. Описание параметров создаваемого поля добавления Active Directory

№	Параметры	Описание
1.	Тип авторизации AD	Базовый – по протоколу LDAP. Kerberos – сетевой протокол безопасной передачи авторизационных данных, включающий проверку их подлинности.
2.	Адрес контроллера домена	Адрес сервера, контролирующего область компьютерной сети.
3.	Сервисная учетная запись	Имя для входа пользователя в формате email адреса.
4.	Домен	Группа объектов, совместно использующих сеть Active Directory.
5.	Область поиска пользователя	Режим поиска уникальных имен в AD. В AD каждой записи назначается DN (distinguished name / уникальное имя).
6.	Использовать SSL	Флаг, активирующий использование протокола шифрования SSL для повышения безопасности.

После ввода данных необходимо нажать кнопку «Сохранить» и удостовериться в том, что созданный домен отобразился в общем списке Active Directory.

Также на вкладке «Active Directory» присутствует возможность редактирования добавленной записи в таблице доменов AD. В открывшемся окне редактирования записи можно загрузить keytab-файл, файл таблицы ключей, содержащий пары имен субъектов Kerberos и зашифрованные ключи, полученные из пароля Kerberos, с помощью специально отведенного поля (Рисунок 13).

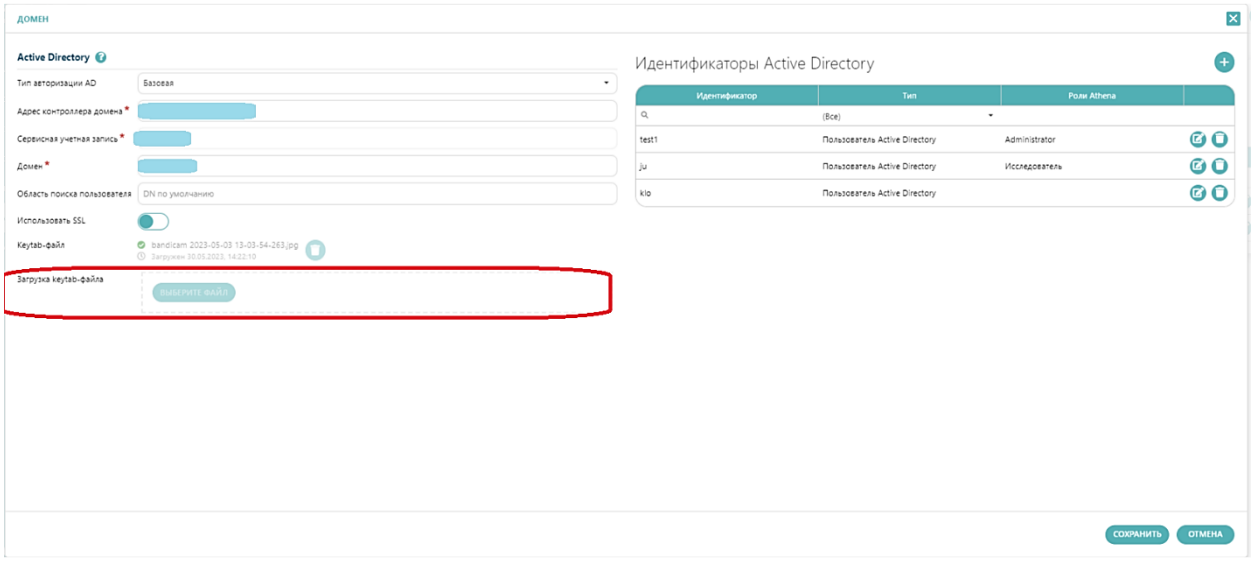

Рисунок 13. Выделенное поле для загрузки keytab-файла

В этом же окне для настройки доступа в Систему, используя учетные записи группы «Active Directory», необходимо нажать кнопку «Добавить». Пример отображения формы добавления идентификатора «Active Directory» представлен ниже (Рисунок 14).

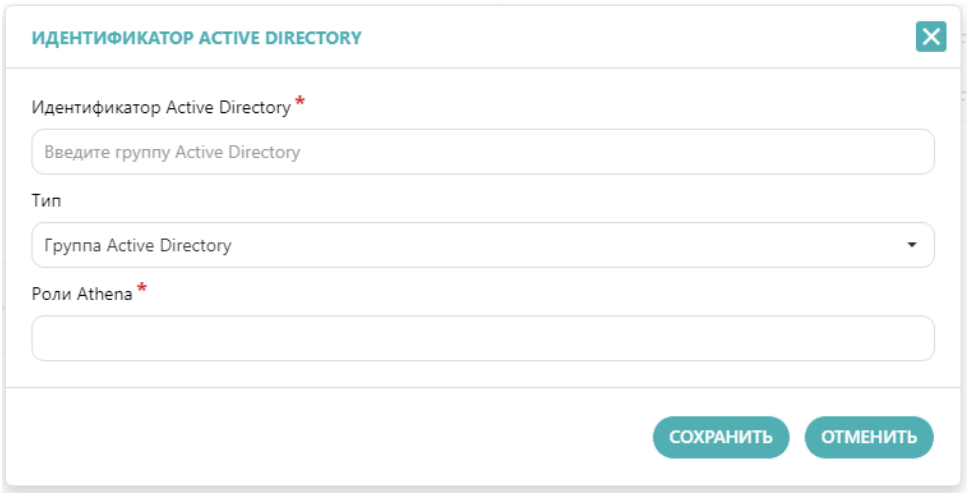

Рисунок 14. Форма «Идентификатор Active Directory»

В отобразившейся форме необходимо указать параметры, описанные в таблице 10.

Таблица 10. Описание параметров создаваемого идентификатора Active Directory

№	Параметры	Описание
1.	Идентификатор Active Directory	Название создаваемой группы Active Directory.
2.	Тип	Типы идентификатора (группа или пользователь).
3.	Роли Athena	Выбор роли из зарегистрированных в системе KAIROS.

После ввода данных необходимо нажать кнопку «Сохранить» и удостовериться в том, что созданный идентификатор отобразился в общем списке настроенных идентификаторов Active Directory.

5.3 Почтовый трафик

Настройка проверки почтового трафика осуществляется во вкладке «Почтовый трафик» (Рисунок 15).

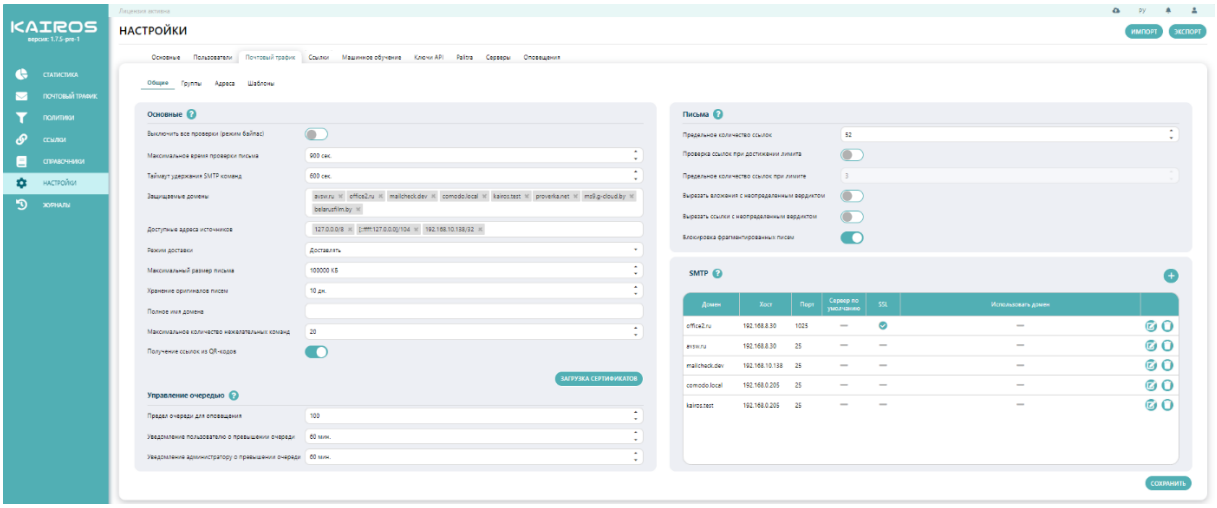

Рисунок 15. Раздел «Настройки», вкладка «Почтовый трафик»

В таблице **11** приведены описания всех настроек данной вкладки:

Таблица 11. Описание настроек почтового трафика

№	Параметры	Описание
1.	Основные	Выключить все проверки (режим байпас) – флаг, при активации которого будет отключен антиспам, проверка заголовков, ссылок и вложений писем Максимальное время проверки письма - период проверки электронных писем с вложениями, при превышении которого приходит оповещение администратору системы Таймаут удержания SMTP команд - время, в течении которого почтовый сервер ожидает ответа на отправленные команды протокола SMTP перед тем, как прервать текущую операцию Защищаемые домены - доступные домены для проверки в системе. Для включения домена в область проверки его нужно указывать полностью, т.к. происходит точное сравнение после знака «@». Например, указание домена office.ru не включает в себя проверку доменов *.office.ru Доступные адреса источников - доступные адреса для проверки писем в системе Режим доставки - поле, указывающее доставлять ли письмо на конечный сервер Максимальный размер письма - максимальный размер письма, доступный для проверки системой Хранение оригиналов писем - время, в течении которого хранятся оригиналы писем в системе Полное имя домена - уникальное имя домена. Включает в себя имена всех родительских доменов иерархии DNS Максимальное количество нежелательных команд - максимальное количество нежелательных команд, при

№	Параметры	Описание
		превышении которого почтовый сервер начнёт блокировать команды Получение ссылок из QR-кодов - сканирование QR-кодов для перехода по ссылкам
2.	Управление очередью	Предел очереди для оповещения — максимальное количество сообщений в очереди, при котором пользователю начинают приходить уведомления Уведомление пользователю о превышении очереди — интервал (мин.), с которым пользователю будут отправляются уведомления о большом количестве сообщений в очереди Уведомление администратору о превышении очереди — интервал (мин.), с которым администратору будут отправляться уведомления о большом количестве сообщений в очереди
3.	Письма	Письма — содержит правила реагирования системы при нестандартных ситуациях проверки Предельное количество ссылок — максимальное количество ссылок в письме, которые будут отправлены на анализ Проверка ссылок при достижении лимита — флаг, при активации которого при превышении предельного количества ссылок в письме, будет проверено количество ссылок, указанное в настройке «Предельное количество ссылок при лимите» Вырезать вложения с неопределенным вердиктом — флаг, при активации которого получатель письма не получит вложение, если ему присвоен вердикт «не определен» Вырезать ссылки с неопределенным вердиктом — флаг, при активации которого получатель письма не получит ссылку, если ей присвоен вердикт «не определен»

№	Параметры	Описание
4.	SMTP	SMTP - содержит настройки SMTP сервера, на который отправляются проверенные письма с вложениями. Хост - IP-адрес или доменное имя сервера SMTP Порт - цифровой идентификатор для инициации соединения с MTA SSL - флаг использования протокола шифрования SSL Логин - логин для авторизации на сервере Пароль - пароль для авторизации на сервере

Данная вкладка имеет следующие категории настроек для почтового трафика, описанные в таблице 12.

Таблица 12. Категории почтовых настроек

№	Категории	Описание
1.	Общие	Общие системные настройки почтового трафика в системе.
2.	Группы	Группы почтовых ящиков клиентов, с предварительно настроенными правилами проверки вложений и оповещения.
3.	Адреса	Почтовые адреса отправителей и получателей, которые участвуют в проверке почтового трафика.
4.	Шаблоны	Шаблоны оповещения различных групп пользователей.

Во вкладке «Общие» присутствует возможность настроить SMTP сервера, на которые отправляются проверенные письма с вложениями. При нажатии на кнопку «Добавить» появится форма для заполнения новой SMTP записи (Рисунок 16).

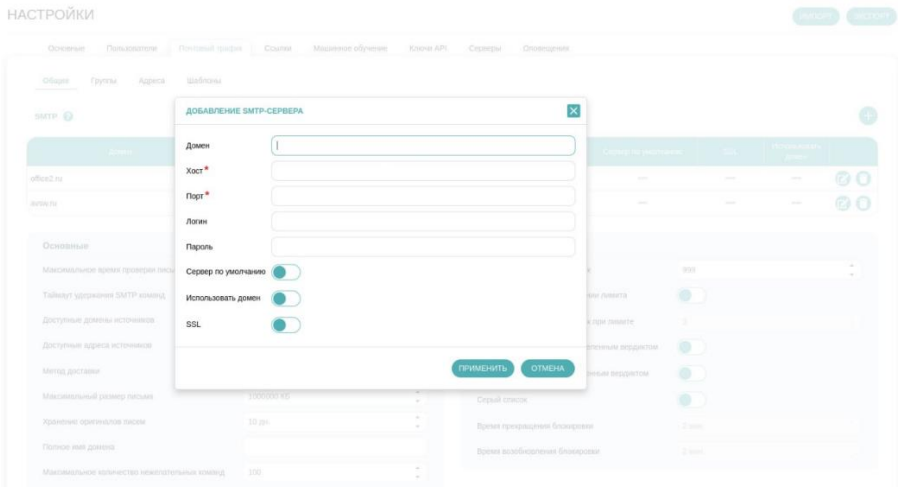

Рисунок 16. Форма «Добавление SMTP-сервера»

Поля добавления новой SMTP записи описаны в таблице 13.

Таблица 13. Описание параметров добавления новой SMTP записи

№	Категории	Описание
1.	Домен	Общие системные настройки почтового трафика в системе.
2.	Хост	IP-адрес или доменное имя сервера SMTP.
3.	Порт	Цифровой идентификатор для инициации соединения с MTA.
4.	Сервер по умолчанию	Флаг, при активации которого будет доставлено сообщение, если есть совпадение записи в поле имени домена. Пример, ранее заданные имя доменов avsw.ru и avsw1.ru не будут является ограничением для строки avsw2.ru и сообщение будет доставлено по умолчанию
5.	SSL	Флаг использования протокола шифрования SSL.
6.	Использовать домен	Отражает статус использования доменов

Есть возможность посмотреть описание каждого параметра настройки, нажав на кнопку описания (Рисунок 17).

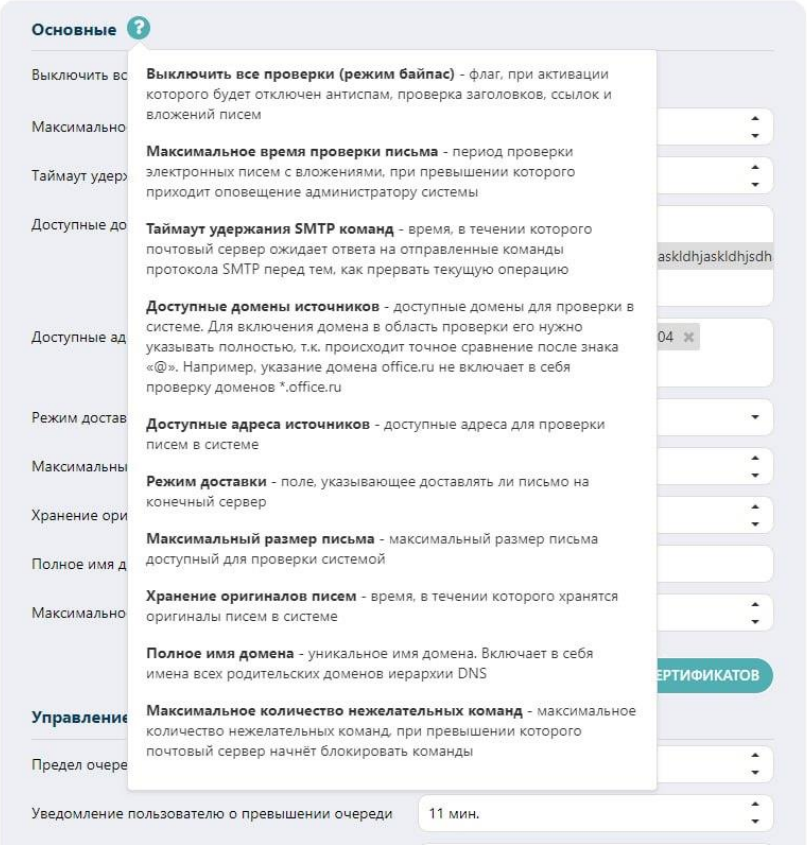

Рисунок 17. Описание основных параметров настройки

Во вложенной вкладке «Общие» присутствуют функциональные блоки с параметрами, описанными в таблице 14.

Таблица 14. Общие параметры настройки почтового трафика

№	Параметры	Описание
1.	SMTP	Настройки SMTP сервера, на который отправляются проверенные письма с вложениями.
2.	Основные	Базовые настройки проверки почтового трафика в системе.
2.1.	Выключить все проверки (Режим байпас)	Выключает/включает все проверки в режиме байпас (Обхода)
2.2.	Максимальное время проверки письма (сек.)	Период проверки электронных писем с вложениями при превышении которого

№	Параметры	Описание
		приходит оповещение администратору системы.
2.3.	Таймаут удержания SMTP команд	Настройка времени удержания SMTP команд
2.4.	Доступные домены источников	Доступные домены для проверки в системе. Для включения в область проверки домена, его нужно указывать полностью, т.к. происходит точное сравнение после знака «@». Например, указание домена office.ru не включает в себя проверку доменов *.office.ru.
2.5.	Доступные адреса источников	Доступные адреса для проверки в системе
2.6.	Метод доставки	Метод доставки почтового трафика из MTA: – Доставлять – Не доставлять – Сохранить локально
2.7.	Хранение оригиналов писем	Настройка времени хранения оригиналов проверяемых почтовых вложений в системе (в днях).
2.8.	Максимальный размер письма	Максимальный вес письма (в байтах). Выставляется в соответствии с настройкой SMTP сервера для ограничения размера приходящего письма.
2.9.	Полное имя домена	Задается полное имя домена
2.10.	Максимальное количество нежелательных команд	Настройка ограничения на количество команд, которые могут быть выполнены клиентом SMTP, прежде чем он будет классифицирован как потенциальный спамер. Нежелательные команды: NOOP, RSET, VRFY и ETRN. При

№	Параметры	Описание
		превышении значения система отклоняет данного клиента.
3.	Управление очередью	
3.1.	Предел очереди для оповещения	Максимальное количество сообщений в очереди, при котором пользователю начинают приходить уведомления.
3.2.	Уведомления пользователю о превышении очереди	Интервал (мин.), с которым пользователю будут отправляются уведомления о большом количестве сообщений в очереди.
3.3.	Уведомление администратору о превышении очереди	Интервал (мин.), с которым администратору будут отправляться уведомления о большом количестве сообщений в очереди.
4.	Письма	Содержит правила реагирования системы в нестандартных ситуациях проверки
4.1.	Предельное количество ссылок	Максимальное количество ссылок в письме, которые будут отправлены на анализ.
4.2.	Проверка ссылок при достижении лимита	Флаг, при активации которого при превышении предельного количества ссылок в письме, будет проверено количество ссылок, указанное в настройке «Предельное количество ссылок при лимите».
4.3.	Предельное количество ссылок при лимите	Максимальное количество ссылок в письме, которые будут проверены при превышении предельного лимита проверки ссылок в письме при включенном флаге «Проверка ссылок при достижении лимита».
4.4.	Вырезать вложения с неопределенным вердиктом	Флаг, при активации которого получатель письма не получит вложение, если ему присвоен вердикт «не определен».

№	Параметры	Описание
4.5.	Вырезать ссылки с неопределенным вердиктом	Флаг, при активации которого получатель письма не получит ссылку, если ей присвоен вердикт «не определен».

5.3.1 Режим обязательной проверки в Системе

Если необходимо настроить проверку почтового трафика «в разрыв», чтобы все письма сначала проходили обязательную проверку в системе, нужно настроить поступление входящей почты на сервер AVSOFT KAIROS, а в методе вывод установить SMTP и целевой сервер, для этого требуется выполнить следующую последовательность действий:

1. Указать почтовые домены, которые принимают электронные письма, включить метод вывода SMTP в следующей директории «Настройки» – «Почтовый трафик» – «Общие» (Рисунок 18).

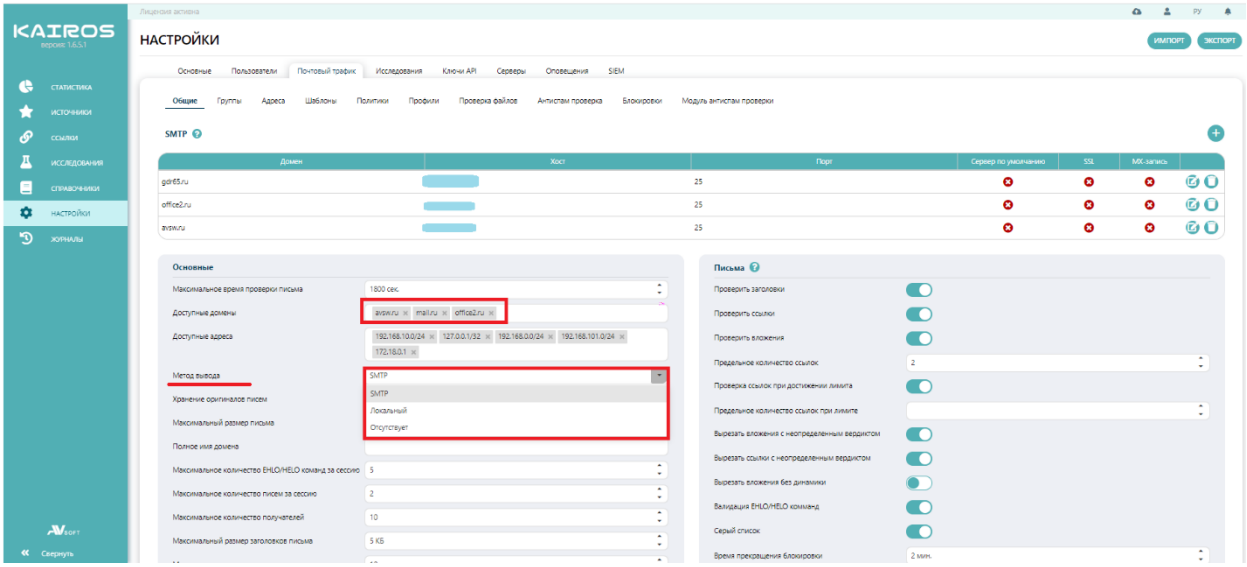

Рисунок 18. Указание домена приема электронных писем

2. Далее необходимо указать адреса, порты и учетные данные серверов, куда будут отправляться письма после проверки нажав на кнопку «Добавить» (Рисунок 19).

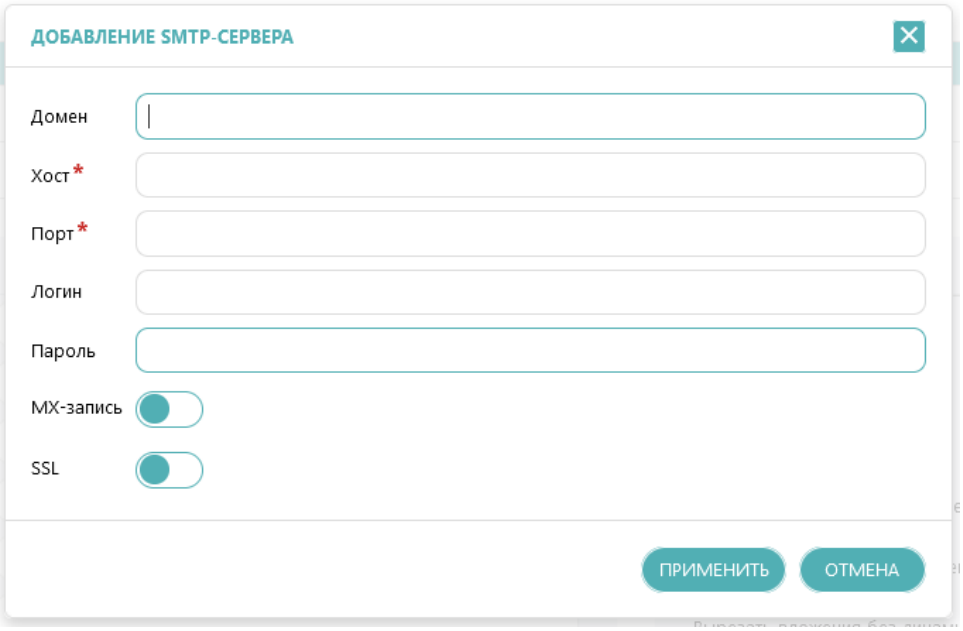

Рисунок 19. Добавление SMTP-Сервера

3. Далее необходимо нажать кнопку «Сохранить».
4. Администратору необходимо изменить точку входа с MTA Заказчика на сервер KAIROS.
5. Открыть 25 порт и выставить настройку без авторизации.

5.3.2 Режим параллельной проверки в системе

Если необходимо настроить проверку почтового трафика в режиме «зеркала» BCC копии трафика, чтобы все письма параллельно проходили проверку в системе, то требуется выполнить следующую последовательность действий:

1. Указать почтовый домен, который принимает электронные письма в следующей директории «Настройки» – «Почтовый трафик» – «Общие» (Рисунок 20).

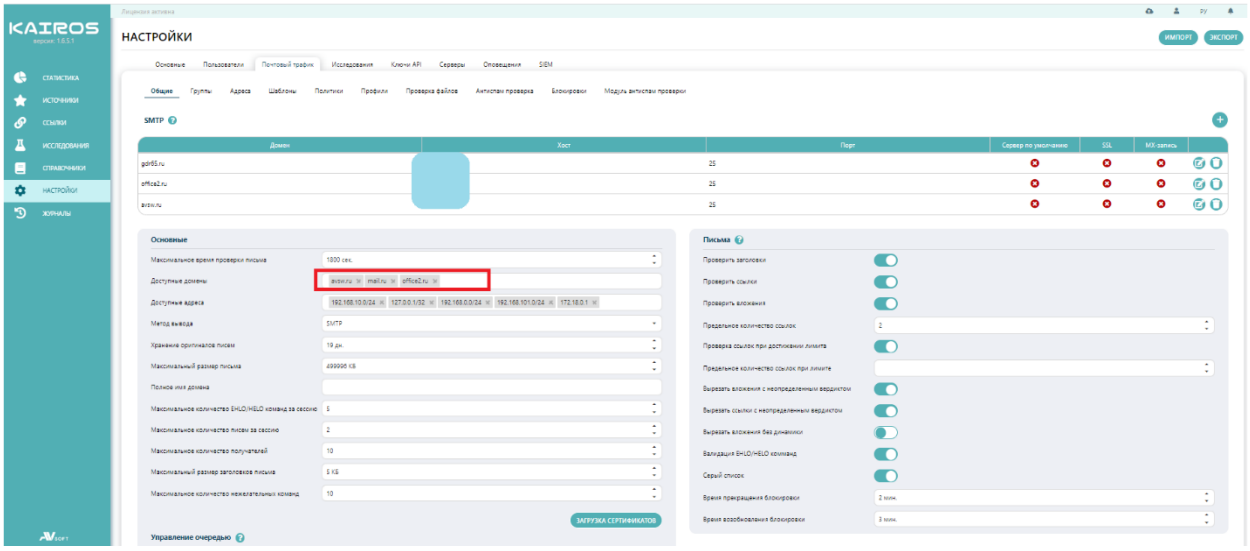

Рисунок 20. Указание домена приема электронных писем

2. Далее необходимо указать метод вывода «Отсутствует» (Рисунок 21).

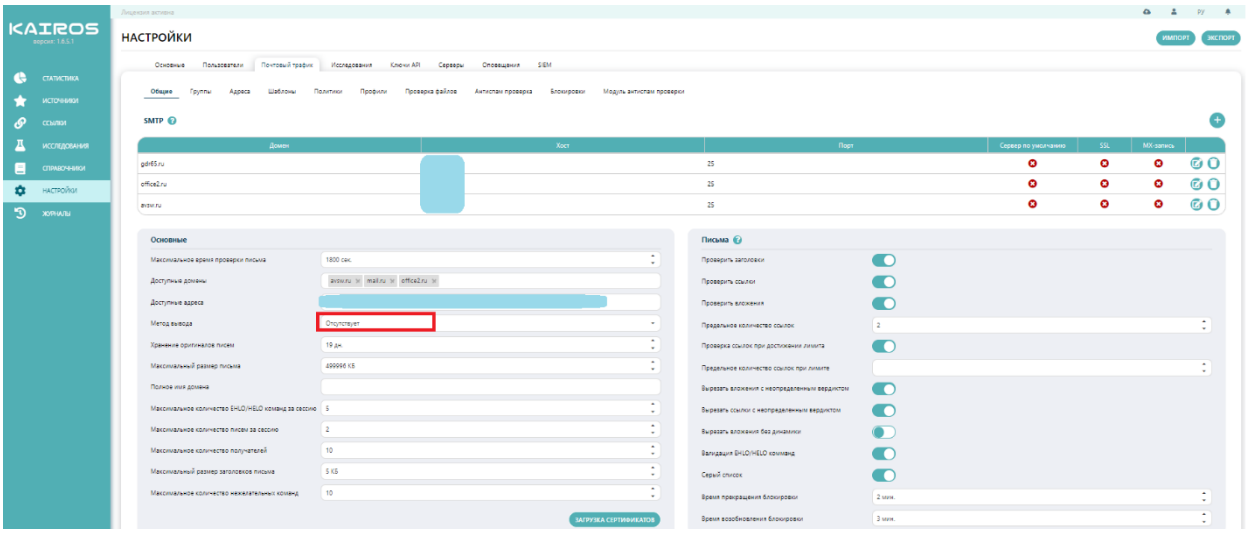

Рисунок 21. Указание метода вывода

3. Далее необходимо нажать кнопку «Сохранить».
4. На MTA заказчика необходимо выполнить следующие настройки:
   - Необходимо указать дополнительный домен нашего сервера AVSOFT KAIROS.
   - Поставить настройку скрытой копии (BCC) и указать в почтовом клиенте MUA организации адрес сервера исходящей почты - AVSOFT KAIROS. Метод аутентификации указывать не требуется. Отправлять через telnet/другую утилиту, которая может передавать данные по tcp.

Режим зеркала является рекомендованным для тестирования корпоративного почтового трафика в Системе.

Для добавления нового домена на проверку в системе необходимо выполнить переход «Почтовый трафик» → «Общие» и в поле «Доступные домены» добавить необходимый тип домена на проверку (Рисунок 22).

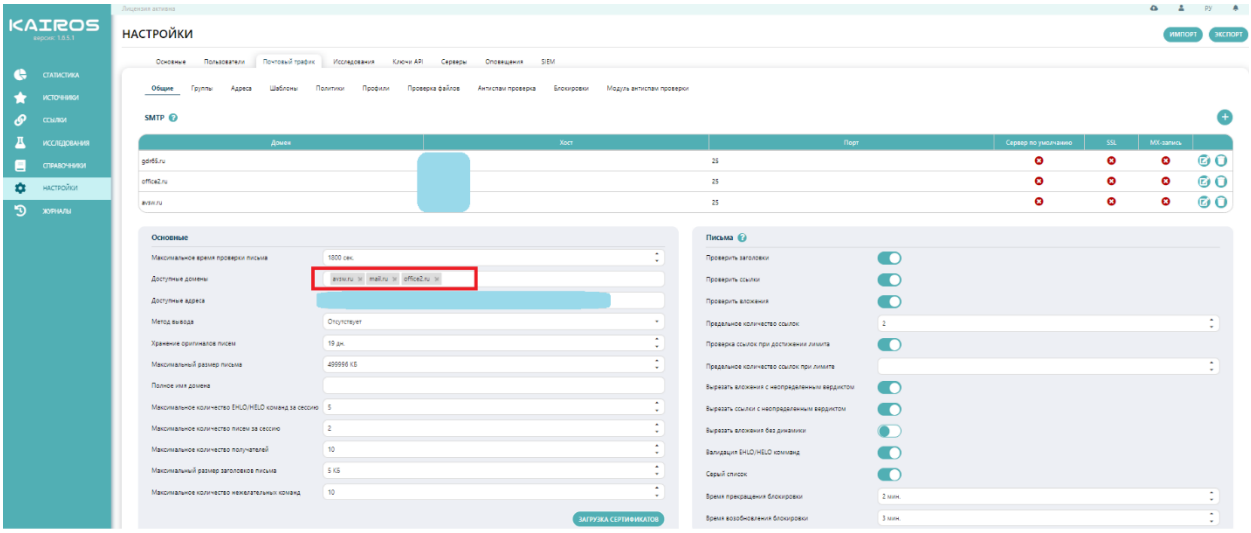

Рисунок 22. Добавление нового домена

> **!** **При добавлении нового домена на проверку в веб-интерфейсе Системы также необходимо выполнить добавление данного домена и на MTA.**

5.3.3 Группы

Во вложенной вкладке «Группы» осуществляется создание и настройка групп пользователей с определенными правилами проверки их электронных писем (Рисунок 23).

Рисунок 23. Группы почтовых пользователей

Для создания новой группы необходимо нажать на кнопку «Добавить», которая отобразит форму для заполнения (Рисунок 24).

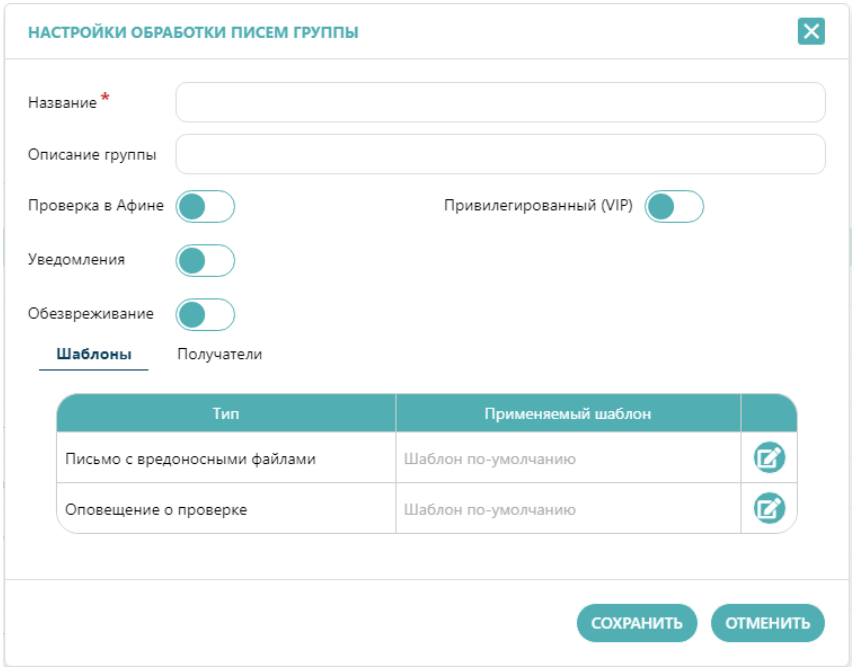

Рисунок 24. Форма «Настройки обработки писем группы»

В окне «Настройка обработки писем группы» необходимо указать параметры, описанные в таблице 15.

Таблица 15. Параметры создания новой группы получателей

№	Параметры	Описание
1.	Название	Название группы получателей электронных писем с вложениями.
2.	Описание группы	Краткое идентификационное описание группы.
3.	Проверка в Афине	Флаг, активирующий функцию проверки электронных писем группы пользователей в Системе.
4.	Уведомления	Флаг, активирующий уведомления пользователей группы получателей, электронные письма которых проходят проверку в Системе.
5.	Привилегированный (VIP)	Флаг, активирующий приоритет проверки электронных письме пользователей группы, если система испытывает нагрузку и большой поток данных идет на проверку.

№	Параметры	Описание
6.	Обезвреживание	Флаг, активирующий удаление активного содержимого из файла, если ему присвоен подозрительный или вредоносный вердикт.
7.	Шаблоны	Заранее созданные текстовые формулировки уведомлений для группы пользователей.
8.	Получатели	Адреса электронных ящиков группы пользователей, для которых осуществляется настройка обработки писем.

После завершения ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новая группа настроек отобразилась в общей таблице.

5.3.4 Адреса

Во вложенной вкладке «Адреса» присутствуют почтовые ящики получателей и отправителей электронных писем в организации (Рисунок 25).

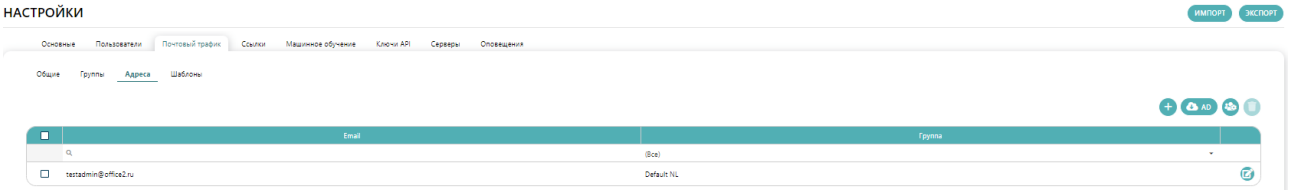

Рисунок 25. Почтовые ящики

Импорт получателей можно осуществить в ручном и автоматическом режиме посредством Active Directory. Для использования функции в ручном режиме необходимо воспользоваться кнопкой «Добавить», которая откроет форму для заполнения «Настройки обработки писем» (Рисунок 26).

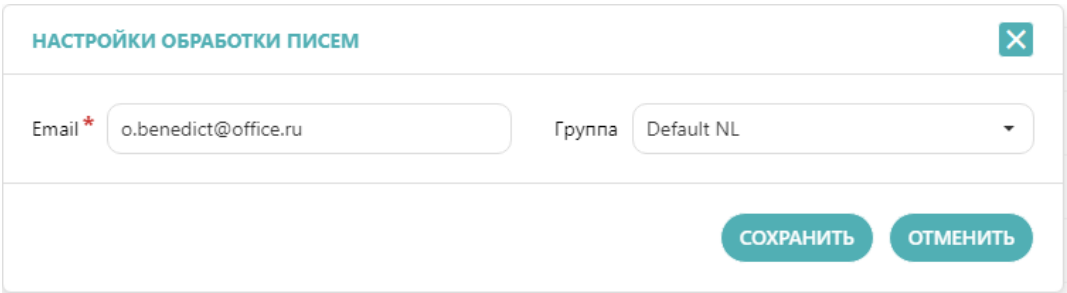

Рисунок 26. Добавление нового получателя

В открывшейся форме необходимо указать электронную почту и группу, к которой будет относиться новый получатель. После завершения ввода

данных необходимо нажать кнопку «Сохранить» и удостовериться, что новый получатель отобразился в общей таблице получателей.

Для импортирования получателей из Active Directory (далее – AD) необходимо нажать на кнопку «Импорт из AD», которая отобразит форму для заполнения «Импорт пользователей из Active Directory» (Рисунок 27).

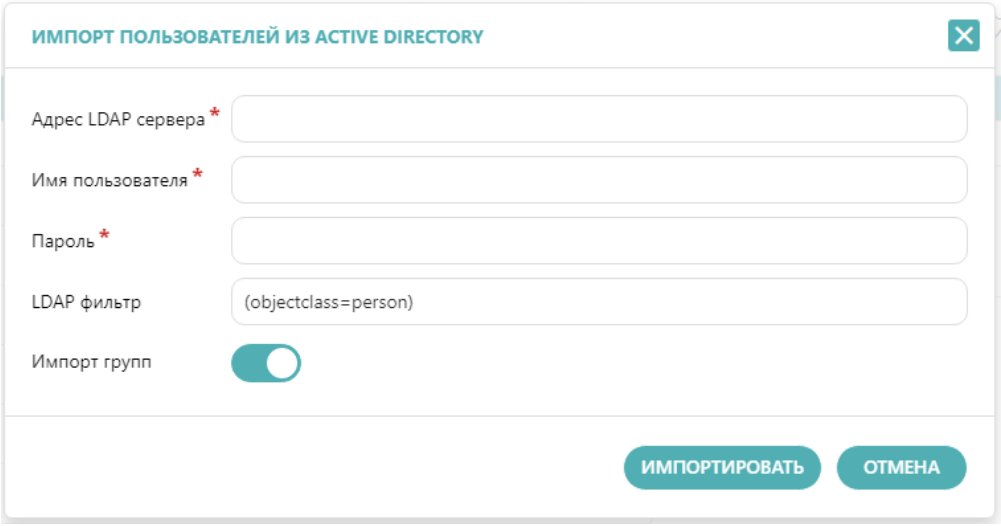

Рисунок 27. Форма «Импорт пользователей из Active Directory»

Для импорта списка пользователей из AD необходимо указать параметры, описанные в таблице 16.

Таблица 16. Параметры импорта из AD

№	Параметры	Описание
1.	Адрес LDAP сервера	Адрес сервера, который осуществляет взаимодействие с AD.
2.	Имя пользователя	Имя пользователя от учетной записи пользователя AD.
3.	Пароль	Пароль от учетной записи пользователя AD.
4.	LDAP фильтр	Фильтр, с помощью которого можно ограничить импорт, например, только пользователями одной группы.
5.	Импорт групп	Если флаг включен, то создадутся отдельные группы для пользователей, как они есть в AD, если выключен, то все попадут в Default.

После завершения ввода данных необходимо нажать кнопку «Импортировать» и удостовериться в общей таблице получателей, что импорт новых получателей осуществлен успешно.

Для добавления получателей в группу необходимо выставить флаги рядом с почтовыми адресами получателей и нажать кнопку «Редактировать группы получателей», расположенную в правом верхнем углу таблицы (Рисунок 28).

Рисунок 28. Таблица «Получатели»

Далее в отобразившейся форме в выпадающем меню необходимо выбрать группу, в которую требуется добавить выбранных пользователей (Рисунок 29).

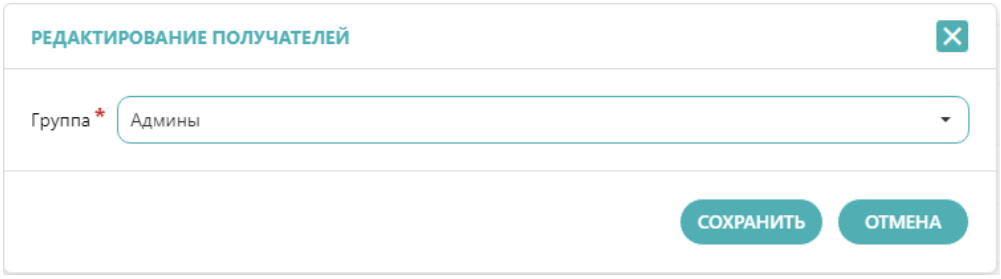

Рисунок 29. Добавление получателей в группы

После завершения ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что выбранные пользователи были добавлены в указанную группу.

5.3.5 Шаблоны

Во вложенной вкладке «Шаблоны» присутствуют шаблоны оповещения по почтовому трафику различных категорий пользователей и администратора системы (Рисунок 30).

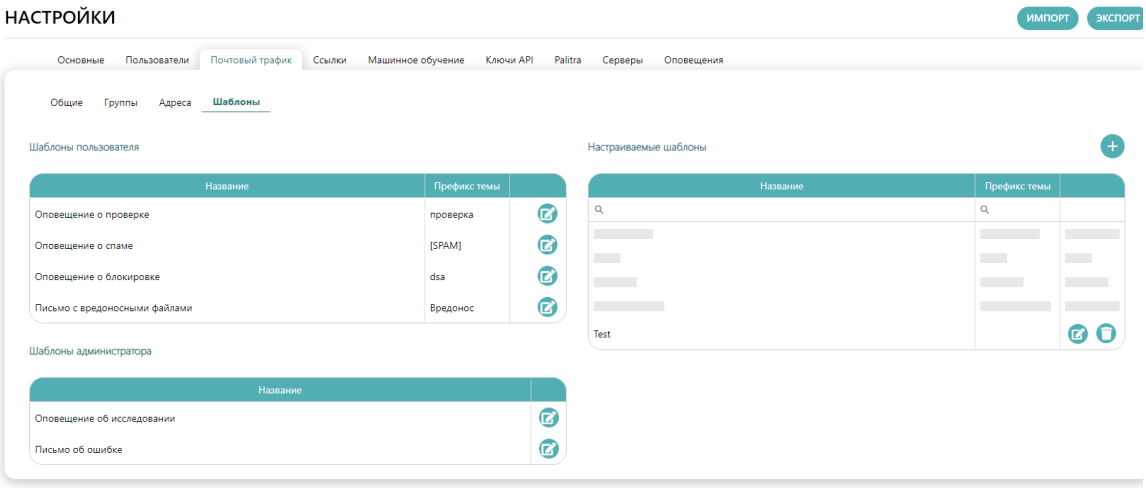

Рисунок 30. Шаблоны уведомлений пользователей

В шаблонах пользователя есть такие готовые шаблоны оповещений, как:

1. Оповещение о проверке;
2. Оповещение о спаме;
3. Оповещение о блокировке;
4. Письмо с вредоносными файлами (содержит информацию о проверке письма и отчет по нему).

В шаблонах администратора по умолчанию имеются готовые шаблоны, которые можно редактировать, нажав иконку «Редактировать», а также создавать новые шаблоны. Для создания нового шаблона необходимо нажать кнопку «Добавить», которая отобразит форму для заполнения «Шаблон» (Рисунок 31).

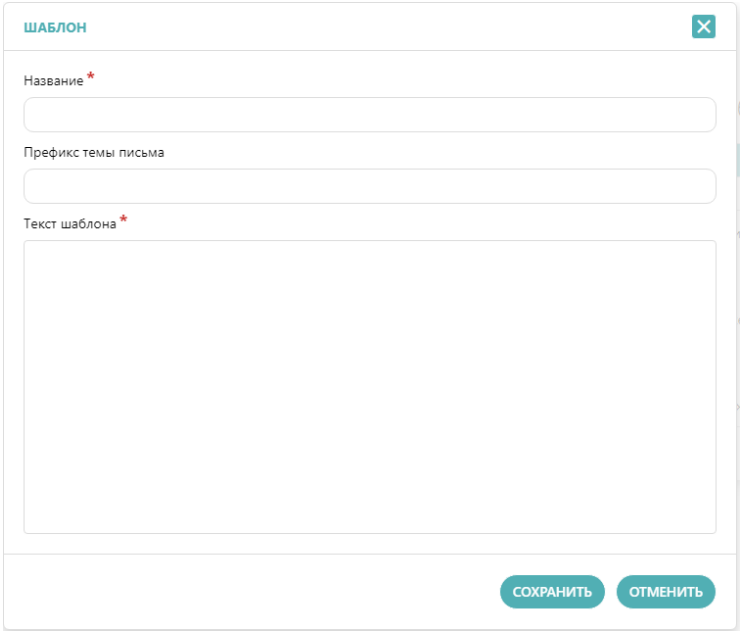

Рисунок 31. Создание нового шаблона

В открывшейся форме необходимо указать параметры, описанные в таблице 17.

Таблица 17. Параметры создания нового шаблона уведомления

№	Параметры	Описание
1.	Название	Название нового шаблона.
2.	Префикс темы письма	Тема, которая будет добавлена перед темой письма, которую указал отправитель.
3.	Текст шаблона	Текст шаблона, который можно дополнять переменными с помощью «@».

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новый шаблон отобразился в общей таблице настраиваемых шаблонов.

Шаблоны имеют функцию редактирования при помощи иконки «Редактировать» (Рисунок 32).

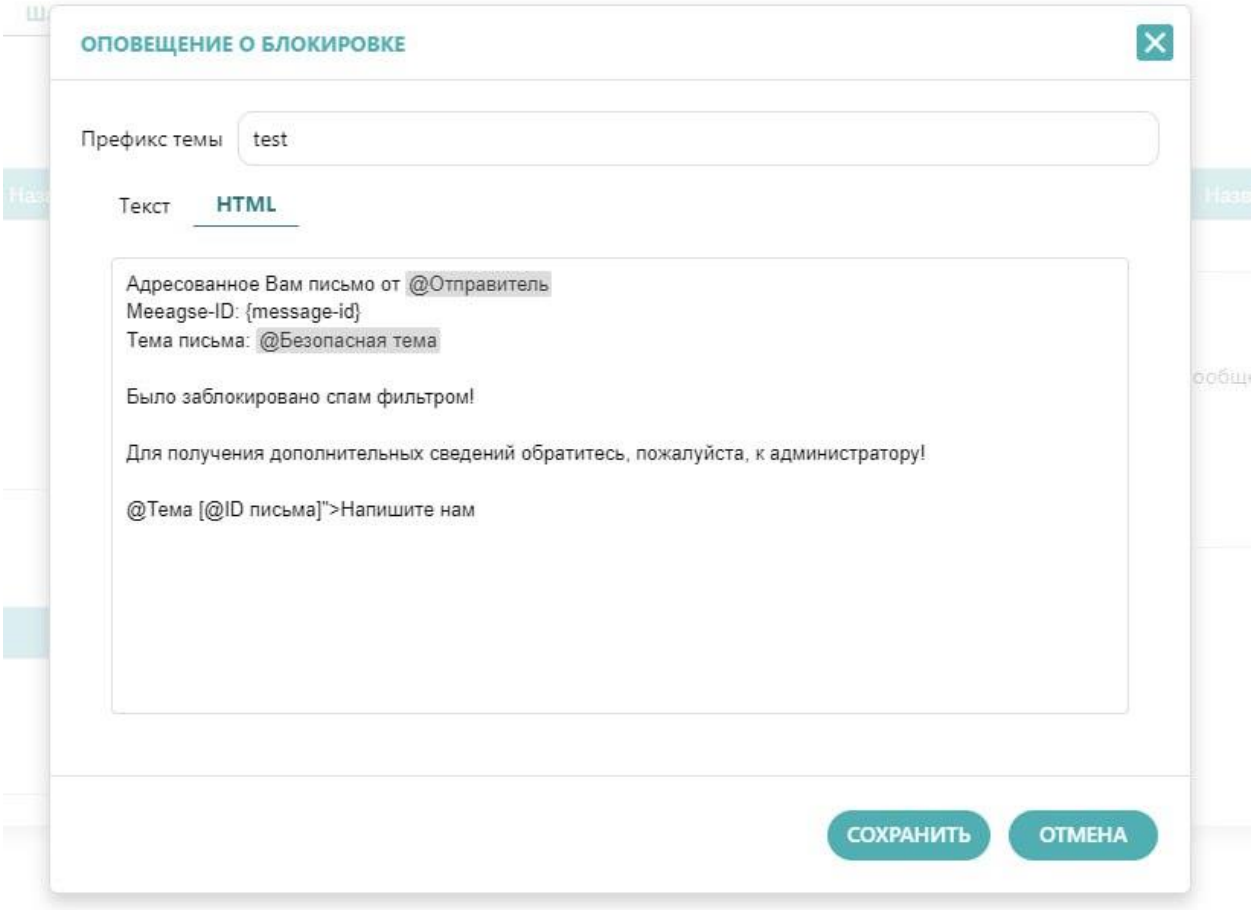

Рисунок 32. Редактирование шаблона «Оповещение о блокировке»

При редактировании шаблона оповещения присутствует опции редактирования текста и переменных. Для использования переменных необходимо в выделенном поле ввести символ «@», далее откроется форма выбора переменной (Рисунок 33).

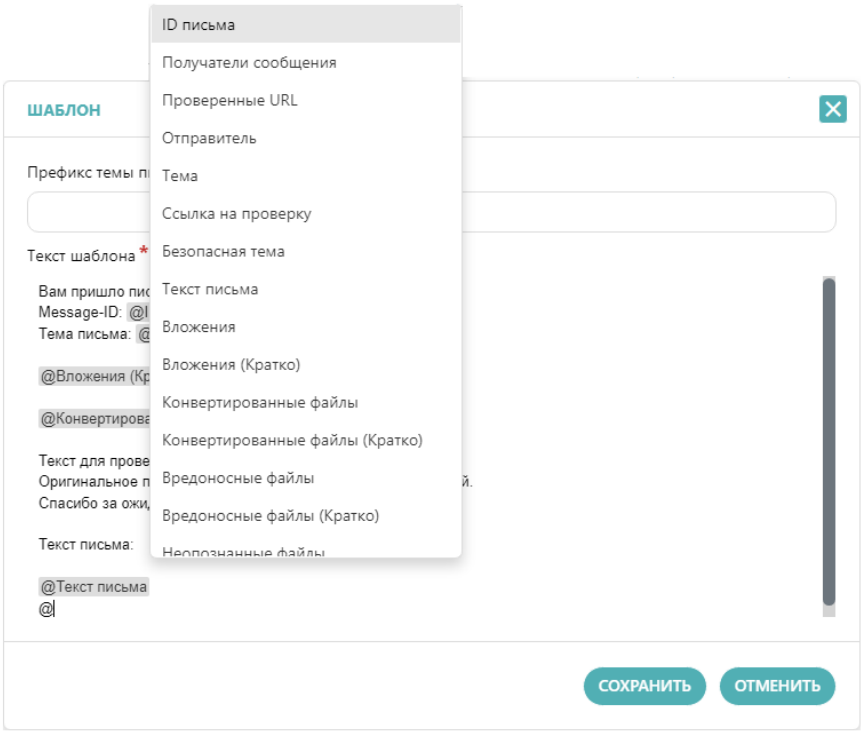

Рисунок 33. Выбор переменной при редактировании шаблона

По окончании корректировки данных необходимо нажать кнопку «Сохранить».

Также имеется возможность добавлять и редактировать HTML-шаблоны для писем (Рисунок 34)

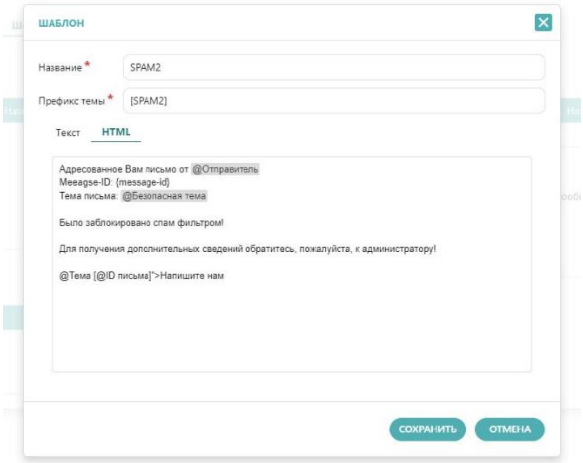

Рисунок 34. HTML-шаблон

5.4 Ссылки

Во вкладке «Ссылки» осуществляется настройка параметров проверки ссылок (Рисунок 35).

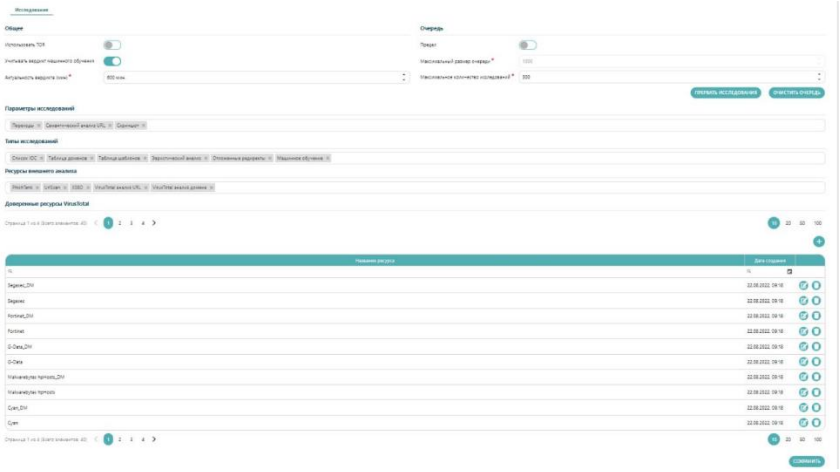

Рисунок 35. Вложенная вкладка «Ссылки»

Параметры вкладки «Ссылки» описаны в таблице 18.

Таблица 18. Настройка параметров проверки ссылок

№	Параметр	Описание	Рекомендация
1.	**Общее**		
1.1.	Использование TOR	Использовать ли сеть TOR при проверке ссылок.	Не рекомендуется для автоматического режима работы системы Рекомендуется для ручных аналитических исследований
1.2.	Учитывать вердикт машинного обучения	Флаг, который отвечает за активацию функции учета вердикта моделей машинного обучения при вынесении общего вердикта по объекту ссылке.	Флаг, рекомендуемый к включению по умолчанию.

№	Параметр	Описание	Рекомендация
1.3.	Актуальность вердикта (мин.)	Время жизни вердикта ссылки, если в течении данного интервала повторно попытаться проверить ссылку, то будет выдан текущий вердикт, если интервал истек, то при повторном запросе вердикта ссылки она будет принудительно перепроверена для актуализации вердикта.	60 минут
2.	**Очередь**		
2.1.	Предел	Флаг, который активирует режим ограничения очереди исследования ссылок на проверку.	Флаг, рекомендуемый к включению по умолчанию, если требуется установка ограничения на обработку большого потока данных, который не может обработать система.
2.2.	Максимальный размер очереди	Параметр позволяет указать максимальный размер очереди исследований на проверку ссылок в системе.	Указывается при активации флага «Предел».
2.3.	Максимальное количество исследований	Максимальное число исследований, которые могут проводиться одновременно.	Выставляется в соответствии с требуемой скоростью проверки ссылок и с техническими

№	Параметр	Описание	Рекомендация
			характеристиками серверного оборудования. По умолчанию – 10.
3.	**Таймауты**		
3.1.	Ответ модуля (мин.)	Временной интервал ожидания ответа от модуля анализа ссылок, при превышении которого будет отображаться ошибка.	30 минут
3.2.	Анализ данных (мин.)	Временной интервал ожидания ответа от модуля анализа данных, при превышении которого отображается ошибка.	10 минут
3.3.	Анализ файлов (мин.)	Временной интервал ожидания ответа от модуля анализа файлов, при превышении которого отображается ошибка.	10 минут

Так же в данном разделе находятся параметры и типы при исследовании ссылок, которые можно добавлять или убирать при необходимости. По окончании ввода данных необходимо нажать кнопку «Сохранить»

Функциональный раздел содержит две кнопки, которые описаны в таблице 19.

Таблица 19. Описание функций кнопок

№	Наименование кнопки	Описание
1.	«Прервать исследования»	Кнопка отвечает за централизованную остановку всех активных исследований ссылок в системе.
2.	«Очистить очередь»	Кнопка отвечает за централизованную отмену всех исследований ссылок в системе, находящихся в очереди.

В этой же вкладке представлен функциональный блок с параметрами работы внешнего аналитического сервиса VirusTotal (Рисунок 36)

Рисунок 36. VirusTotal

Функциональный раздел содержит настройки, которые описаны в таблице 20.

Таблица 20. Параметры настройки VirusTotal

№	Параметры	Описание
1.	Режим	В выпадающем меню можно выбрать варианты взаимодействия с сервисом или отключить его.
2.	**Доверенные**	
2.1.	Антивирусы VirusTotal	Антивирусы VirusTotal, поддерживаемые известными вендорами и показывающие высокую степень детектирования вредоносного ПО. В таблице приведен список антивирусов, которым была

№	Параметры	Описание
		присвоена категория доверенных в системе ATHENA.
2.2.	Ресурсы ссылок	В таблице приведен список ресурсы ссылок, которым была присвоена категория доверенных в системе.

Также присутствует возможность добавлять доверенные антивирусы и ресурсы ссылок, которые используются в работе. Для этого необходимо нажать на кнопку «Добавить». Далее осуществится переход в форму для заполнения (Рисунок 37 и Рисунок 38).

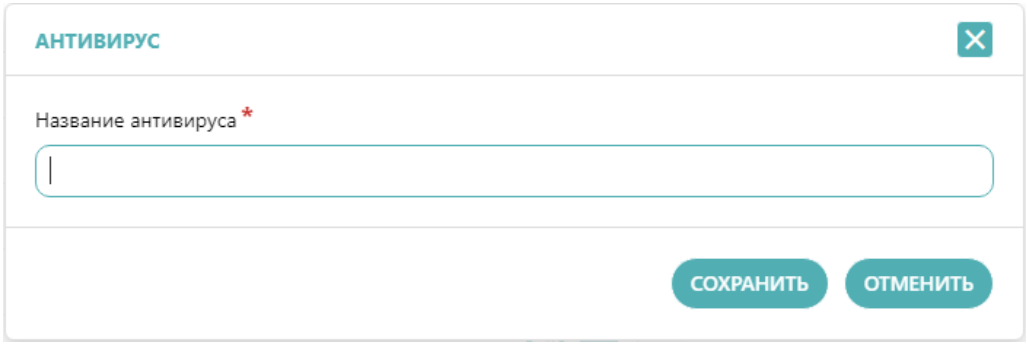

Рисунок 37. Добавление доверенного антивируса

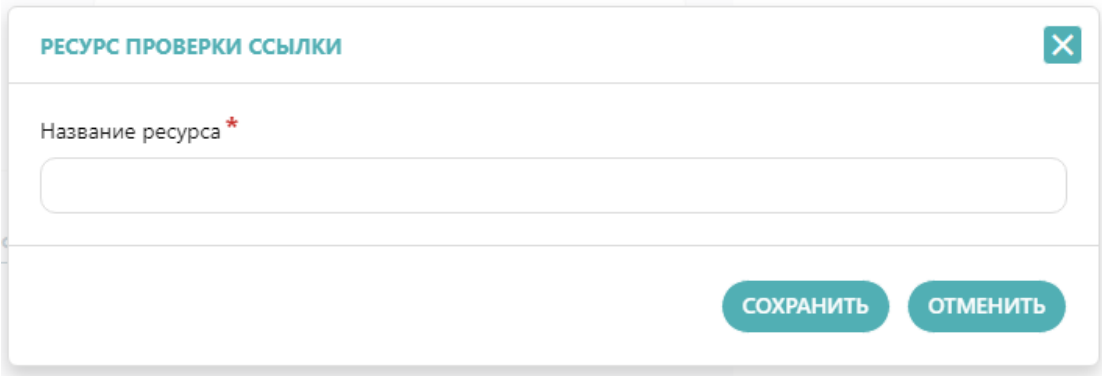

Рисунок 38. Добавление доверенных ресурсов ссылок

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новый антивирус или ресурс ссылки отобразился в общей таблице доверенных.

5.5 Машинное обучение

Вложенная вкладка «Машинное обучение» содержит информацию по настройкам моделей машинного обучения в системе (Рисунок 39).

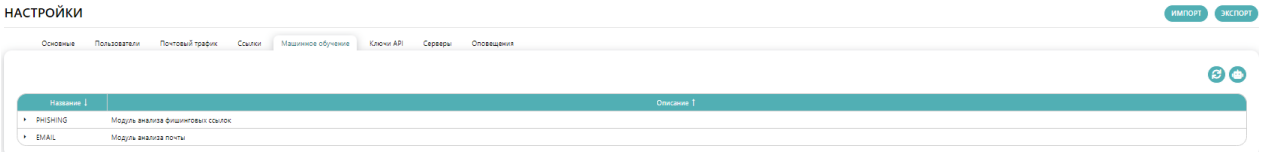

Рисунок 39. Настройки машинного обучения

В общей таблице присутствуют типы моделей машинного обучения, поддерживаемые в системе для анализа. При нажатии на раскрывающееся меню отображаются активные иконки настроек моделей

При нажатии на иконку «Настройки» отображается окно «Настройки модели» (Рисунок 40).

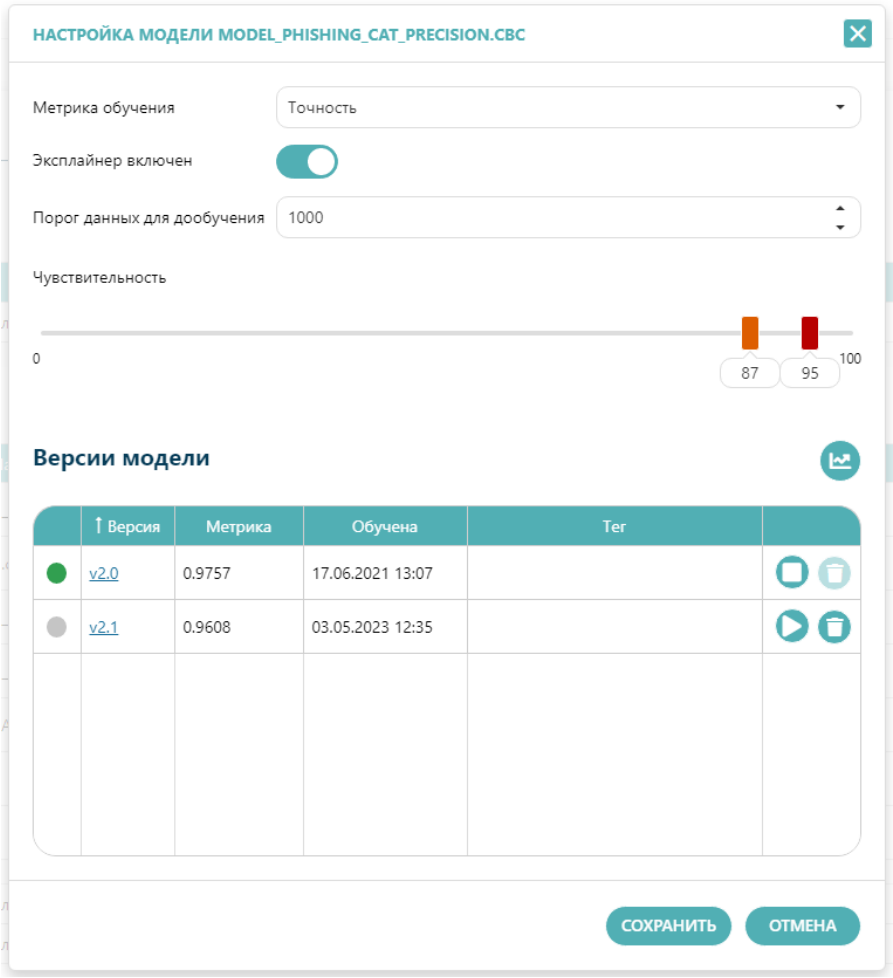

Рисунок 40. Настройки модели машинного обучения

В открывшейся форме представлены настройки, описанные в таблице 21.

Таблица 21. Параметры настройки модели ML

№	Параметры	Описание
1.	Метрика обучения	Параметр оценки качества модели ML. В выпадающем списке выбирается метрика, на основании которой выбирается оценка соответствия модели функциям применения.
2.	Эксплайнер включен	Флаг, активирующий отображение объясняющего графика рядом с моделью ML в отчете по проверке.
3.	Порог данных для дообучения	Количество файлов, которые рекомендуется предварительно собрать ботам для активации процесса дообучения модели.
4.	Чувствительность	Пороговые значения оценки вердикта ссылки.
5.	Версии	Версии модели ML и основная информация по ним.

После завершения ввода данных необходимо нажать кнопку «Сохранить».

Система поддерживает функцию дообучения у определенных типов моделей ML, если данная функция поддерживается, то в строке модели отображается иконка «Обучить». При нажатии на иконку «Обучить» отображается окно «Переобучение модели» (Рисунок 41), в котором необходимо выбрать метрику обучения, период данных для обучения и выставить тег (опциально).

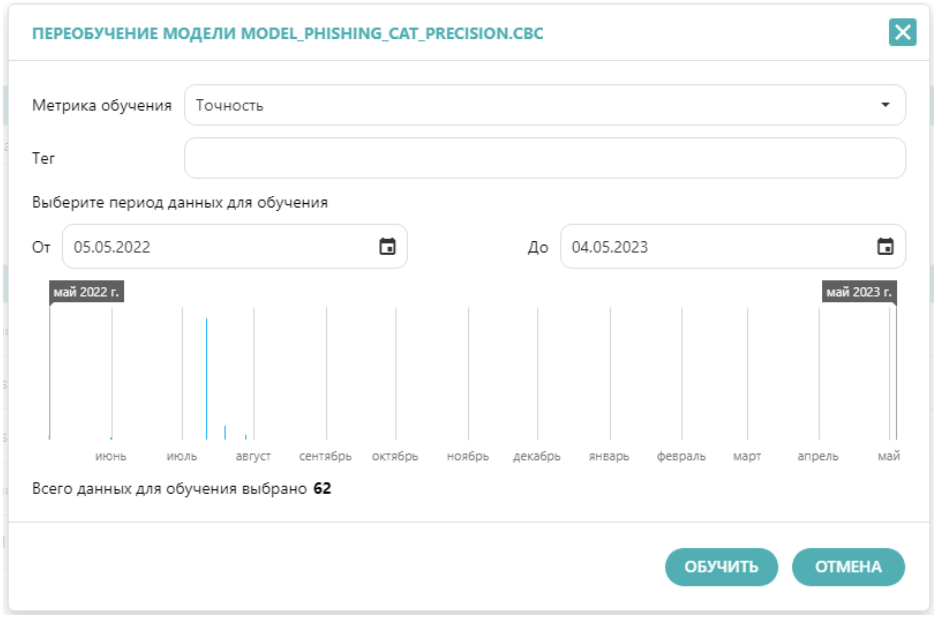

Рисунок 41. Параметры переобучения модели ML

После выставления параметров обучения необходимо нажать на кнопку «Обучить» и удостоверится, что система отобразила уведомление об успешной отправке на дообучение выбранной модели.

5.6 Ключи API

Во вкладке «Ключи API» присутствует информация по всем API ключам, используемым в системе для взаимодействия с внутренними модулями и внешними системами (Рисунок 42).

В таблице есть возможность сортировать и фильтровать состояние ключей.

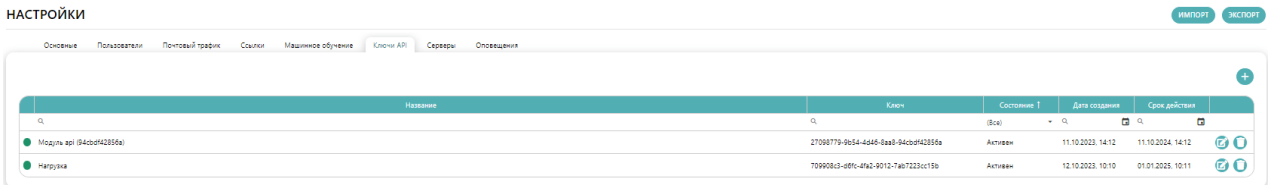

Рисунок 42. Ключи API

Для создания нового API ключа необходимо воспользоваться кнопкой «Добавить», которая отобразит окно «Настройки ключей API» (Рисунок 43).

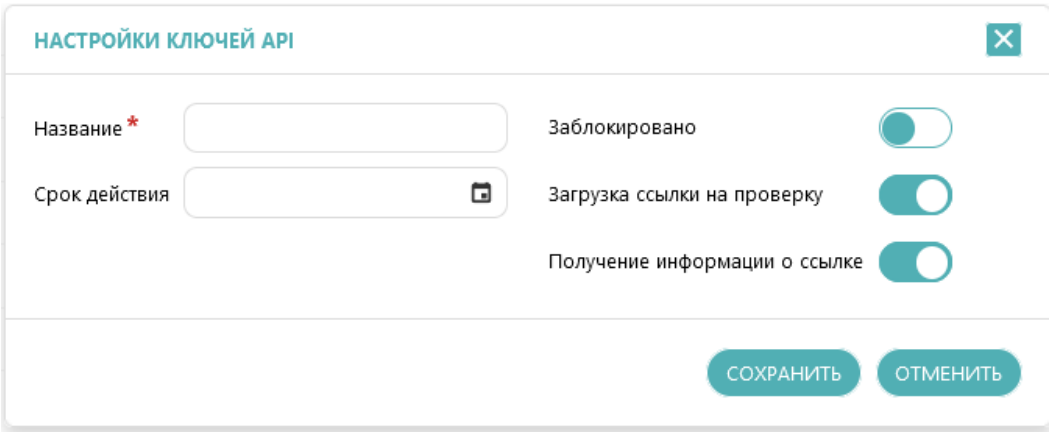

Рисунок 43. Создание нового ключа API

В открывшейся форме необходимо указать название сервиса, для которого необходим ключ, и срок действия API ключа. После завершения ввода данных необходимо нажать кнопку «Сохранить».

5.7 Palitra

Вкладка «Palitra» позволяет подключить соединение Системы с системой централизованного управления и мониторинга PALITRA. Для этого нужно внести адрес подключения и посмотреть статус подключения (Статус должен быть «Подключено») (Рисунок 44)

Рисунок 44. Подключение Palitra

5.8 Серверы

Вкладка «Серверы» содержит информацию по всем зарегистрированным сервисам в Системе.

Вложенная вкладка «Мониторинг» содержит описание модулей системы, уровень важности каждого модуля, их готовность к работе (Рисунок 45). Для просмотра полной информации по модулю системы и ее редактирования необходимо нажать на стрелочку слева от нужного модуля.

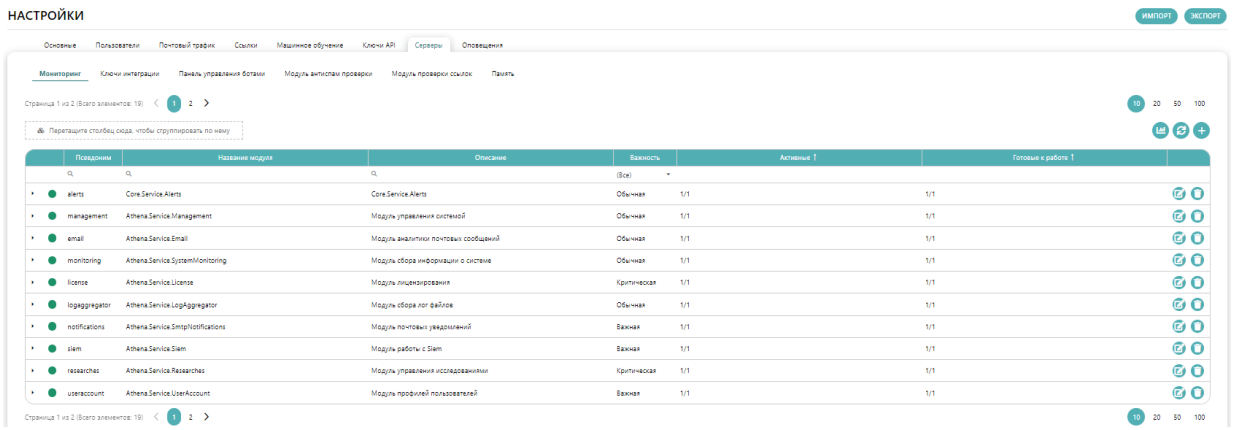

Рисунок 45. Вложенная вкладка «Мониторинг»

В открывшемся меню указана следующая актуальная информация по модулю Системы:

– IP-адрес модуля

– Порт модуля

– Версия модуля

– Дата изменения модуля

– Быстрая проверка модуля и ее дата

– Функциональная проверка модуля и ее дата.

При необходимости корректировки данных модуля системы необходимо воспользоваться иконкой «Редактировать» справа от подробной информации по модулю. Система предоставляет возможность удаления неактуальных модулей. Для этого следует нажать на иконку «Удалить» напротив выбранного модуля.

Для добавления нового модуля необходимо нажать кнопку «Добавить». Далее осуществится переход во всплывающее окно для заполнения «Объект мониторинга» (Рисунок 46).

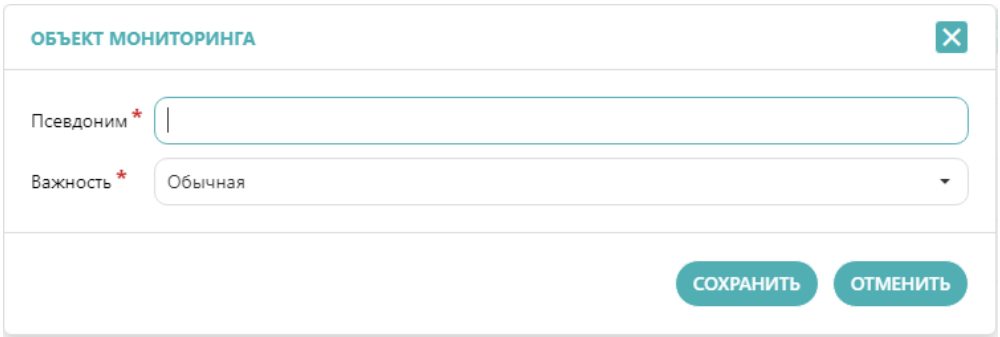

Рисунок 46. Добавление объекта мониторинга

В поле «Псевдоним» необходимо указать наименование объекта и в поле «Важность» в выпадающем меню выбрать уровень важности с точки зрения оповещения. По завершении ввода данных необходимо нажать кнопку «Сохранить».

Для просмотра журнала работоспособности модулей необходимо нажать на кнопку «Журнал работоспособности». Далее на экране отобразится окно «Журнал работоспособности» (Рисунок 47).

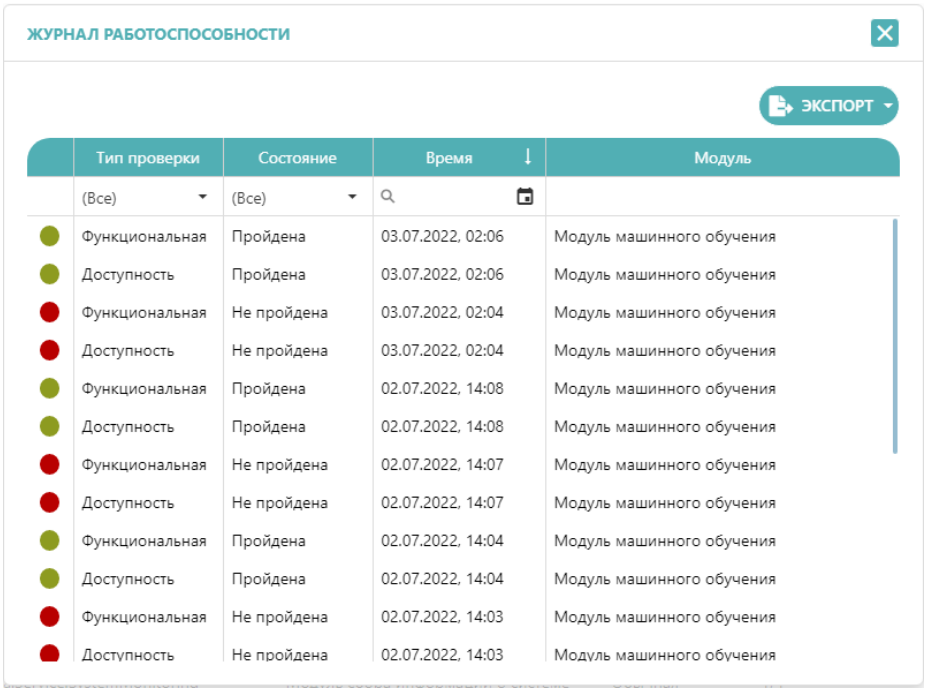

Рисунок 47. Окно «Журнал работоспособности»

В данном окне отображается следующая информация о модулях системы. Для выгрузки журнала работоспособности предназначена кнопка «Экспорт».

> **! Добавление новых модулей осуществляется инженерами компании АВ Софт.**

Во вложенной вкладке «Ключи интеграции» присутствуют настройки ключей интеграции, которые используются для интеграции с другими сервисами (Рисунок 48).

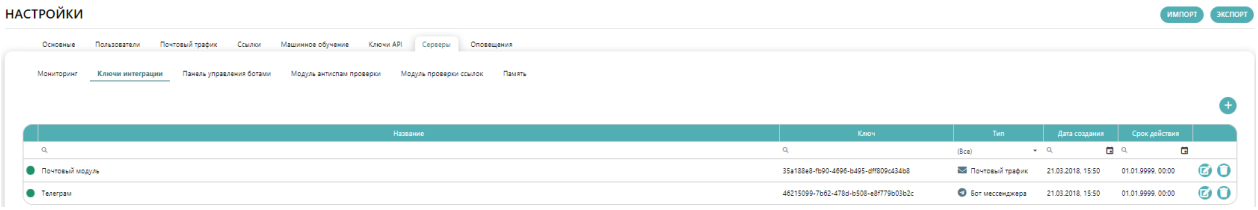

Рисунок 48. Вложенная вкладка "Ключи интеграции"

Для добавления нового ключа необходимо нажать на кнопку Добавить». Далее осуществится переход в форму «Настройки ключей интеграции» (Рисунок 49).

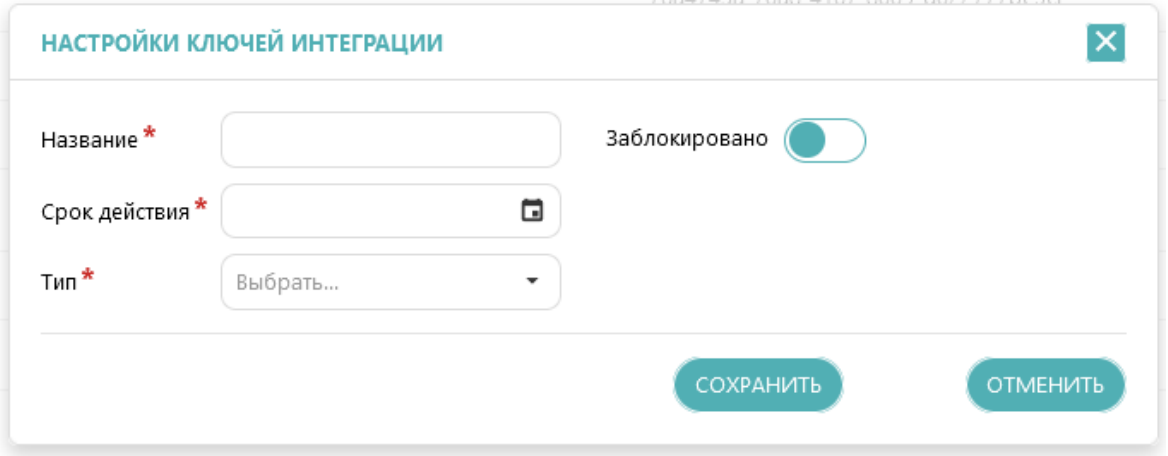

Рисунок 49. Форма "Настройки ключей интеграции"

В открывшейся форме необходимо ввести параметры, описанные в таблице 22.

Таблица 22. Параметры формы "Настройка ключей интеграции"

№	Параметры	Описание
1.	Название	Название ключа.
2.	Срок действия	Срок действия ключа
3.	Тип	Тип ключа интеграции.
4.	Заблокировано	Флаг блокировки ключа

Далее необходимо нажать кнопку «Сохранить» и убедиться, что добавленная настройка появилась в общей таблице ключей интеграции.

Во вложенной вкладке «Панель управления ботами» присутствуют настройки управления ботами, которые собирают различные значимые с точки зрения анализа вредоносного объекта данные (Рисунок 50).

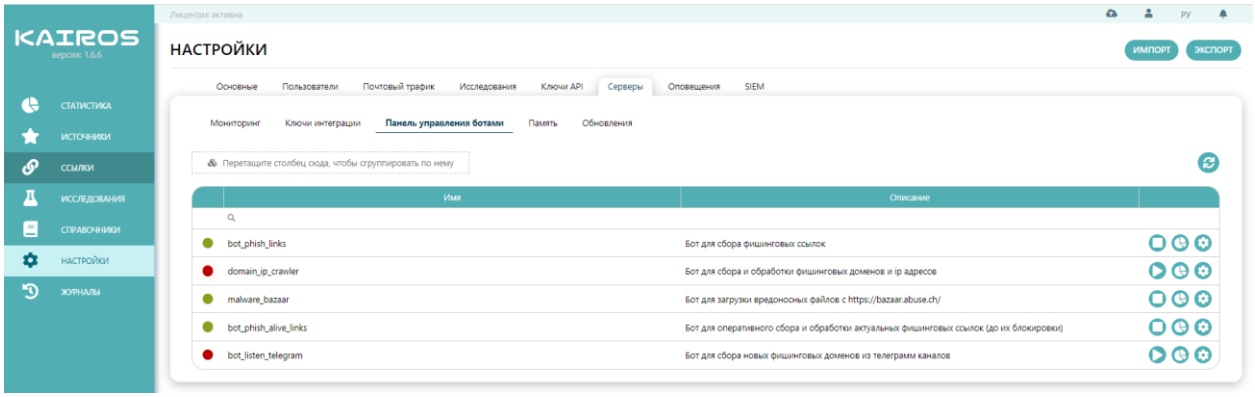

Рисунок 50. Панель управления ботами

Для остановки работы бота необходимо нажать на иконку «Остановить», для запуска – «Запустить».

Для просмотра статистики по работе бота необходимо нажать на иконку «Графики», которая отобразит форму «Статистика» (Рисунок 51).

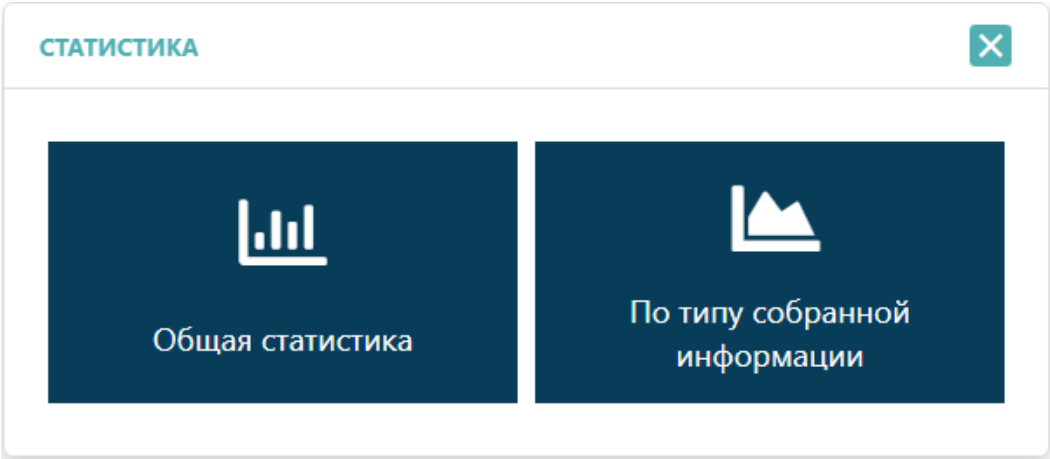

Рисунок 51. Форма «Статистика»

Далее необходимо выбрать тип отображаемых статистических данных (Рисунки 52 - 53).

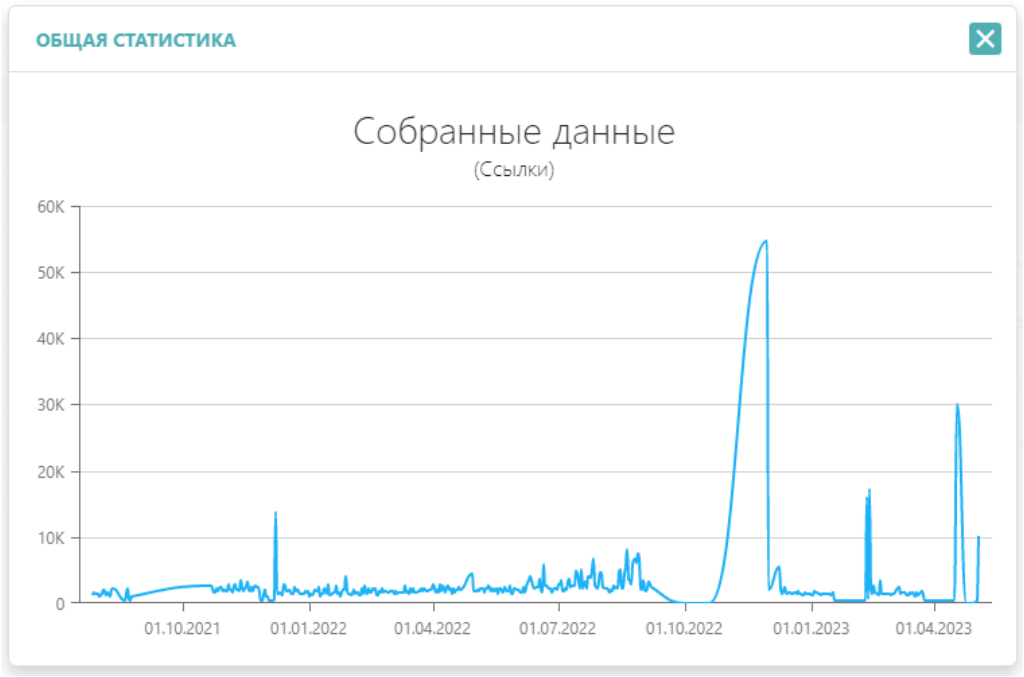

Рисунок 52. Общая статистика

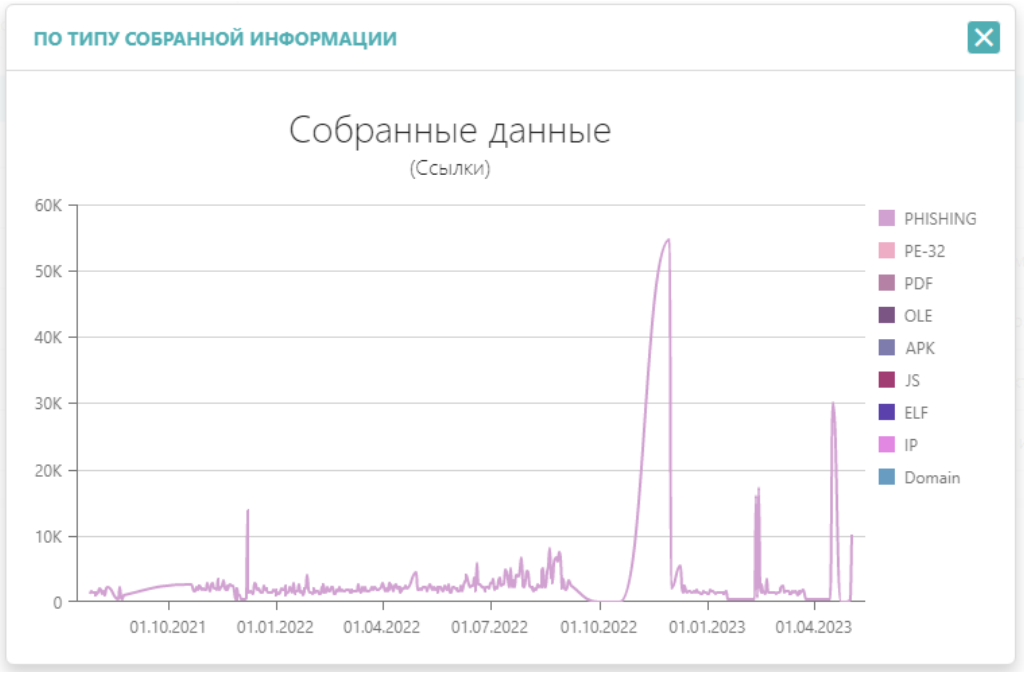

Рисунок 53. Статистика по типам собранной информации

Во вкладке «Модуль проверки ссылок» находится информация о хостах, портах и версиях антиспам проверок. Есть возможность настройки проверки (Рисунок 54).

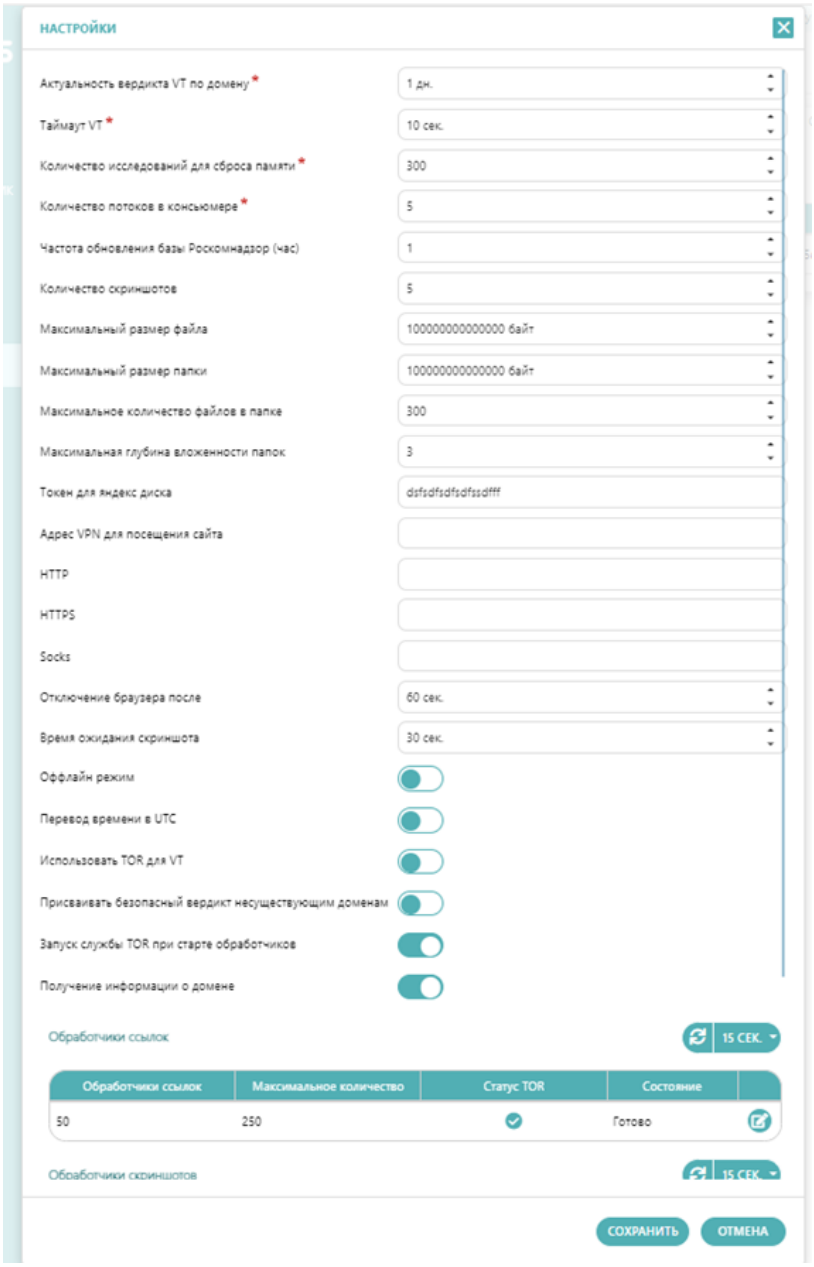

Рисунок 54. Модуль проверки ссылок

Во вкладке «Модуль антиспам проверки» можно посмотреть адрес, порт и версию антиспам сигнатур. Модуль можно обновить (Рисунок 55)

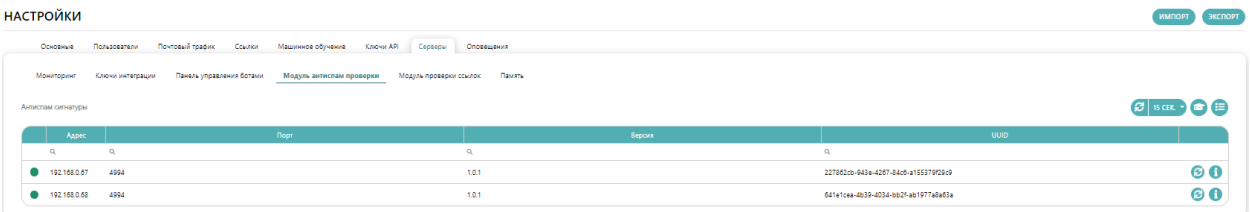

Рисунок 55. Модуль антиспам проверки

Во вложенной вкладке «Память» присутствуют параметры настройки хранения собираемых лог-файлов в системе (Рисунок 56).

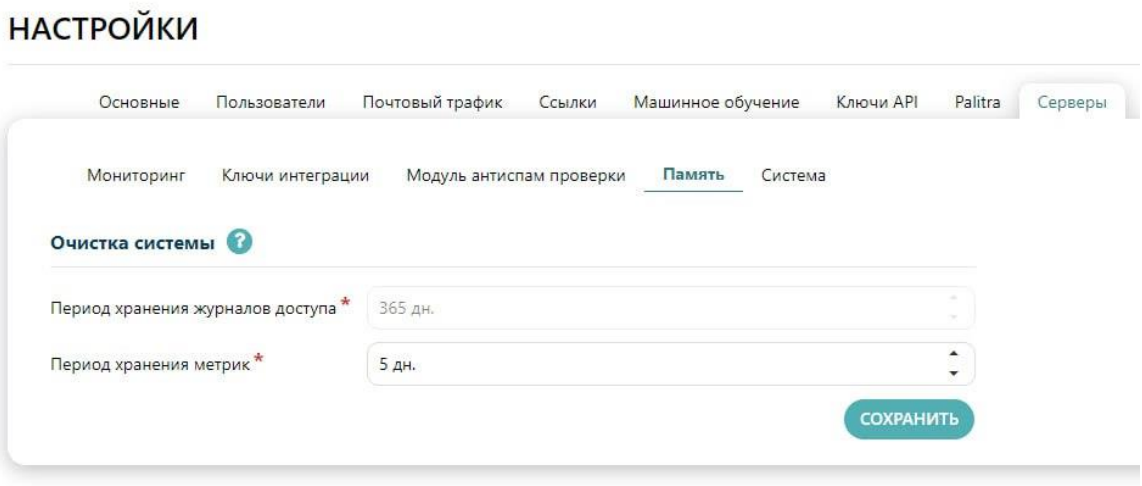

Рисунок 56. Вложенная вкладка «Память»

Описание параметров раздела «Память» представлено в таблице 23.

Таблица 23. Параметры настройки управления памятью

№	Параметры	Описание
1.	**Очистка системы**	
1.1.	Период хранения журналов доступа	Период, за который журналы доступа не будут удалены при запуске автоматической очистки системы
1.2.	Период хранения метрик	Период хранения данных для графиков

Во вложенной вкладке «Система» отображаются данные по системам, подключенным к основной (Рисунок 57)

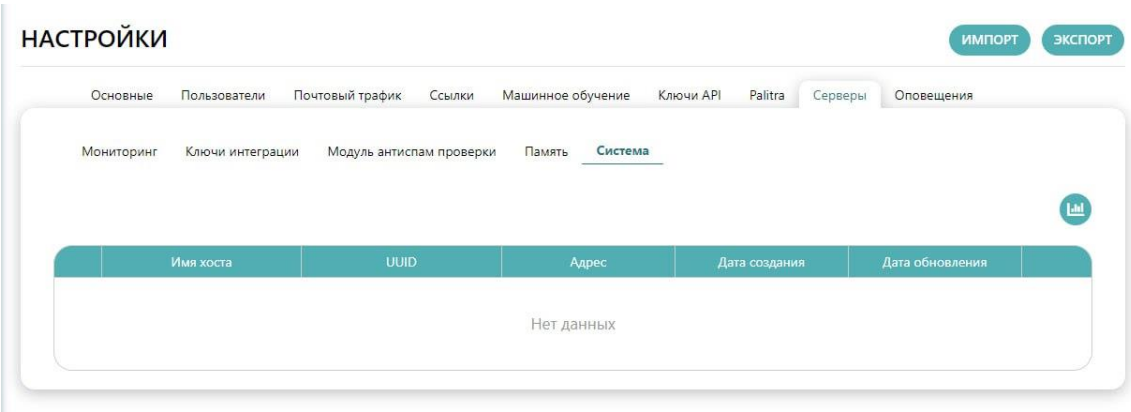

Рисунок 57. Данные о системах

5.9 Оповещения

Вкладка «Оповещения» содержит информацию по оповещению администратора по значимым параметрам в работе Системы (Рисунок 58).

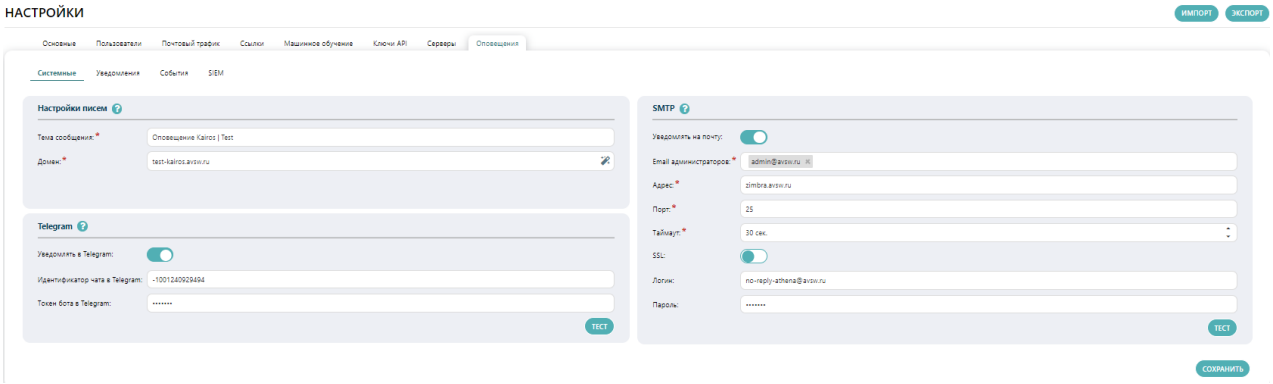

Рисунок 58. Настройка системных оповещений для администратора

Вложенная вкладка «Системные» содержит функциональные блоки по настройке писем, SMTP и Telegram канала, описанные в таблице 24.

Таблица 24. Настройка системных оповещений

№	Настройки	Описание
1.	**Настройки писем**	
1.1.	Тема сообщения	Тема в электронном письме оповещения администратора.
1.2.	Домен	Домен оповещения администратора.
2.	**Telegram**	
2.1.	Уведомлять в Telegram	Флаг, активирующий уведомление в аккаунт Telegram. Рекомендуется к использованию для оперативного получения информации по состоянию системы.
2.2.	Идентификатор чата в Telegram	Персональный Telegram User ID, который можно узнать в специализированных ботах сервиса Telegram (например «What’s my Telegram ID?» и подобных).
2.3.	Токен бота в Telegram	Администратору Системы надо указать токен своего бота в Telegram.

№	Настройки	Описание
2.4.	Тест	Кнопка отправки тестового сообщения, которую необходимо использования после сохранения настроек кнопкой «Сохранить».
3.	**SMTP**	
3.1.	Уведомлять на почту	Флаг, активирующий уведомление администратора по электронной почте.
3.2.	Email администраторов	Электронные почты администраторов системы, которых необходимо уведомлять о системных инцидентах.
3.3.	Адрес	Доменный адрес SMTP сервера.
3.4.	Порт	Открытый порт SMTP сервера для взаимодействия.
3.5.	Таймаут	Временной интервал (в секундах) повторной отправки уведомления об инциденте системному администратору.
3.6.	SSL	Флаг, активирующий использование протокола шифрования SSL. Рекомендуется к использованию для повышения безопасности обмена данными.
3.7.	Логин	Логин от учетной записи на SMTP сервере.
3.8.	Пароль	Пароль от учетной записи на SMTP сервере.
3.9.	Тест	Кнопки отправки тестового письма, которую необходимо использования после сохранения настроек кнопкой «Сохранить».

Вложенная вкладка «Уведомления» содержит информацию по созданию шаблонов уведомлений пользователям Системы (Рисунок 59).

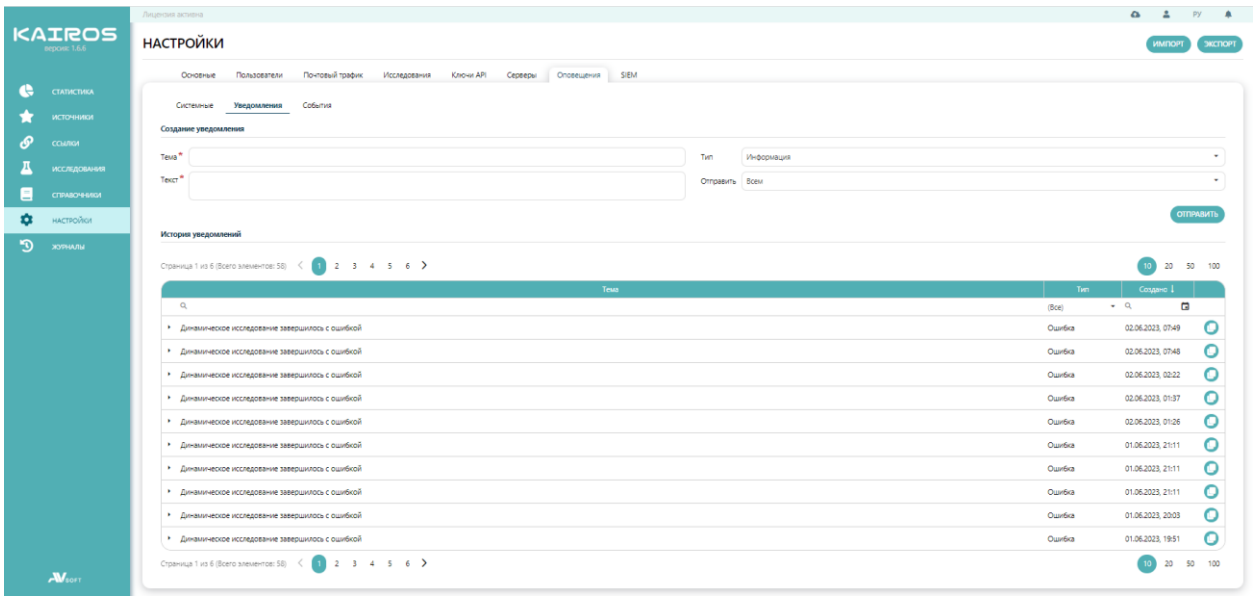

Рисунок 59. Настройка уведомлений пользователей

Для создания уведомления необходимо воспользоваться функциональным блоком «Создание уведомления» и заполнить поля, описанные в таблице 25.

Таблица 25. Параметры создания уведомлений

№	Поля	Описание
1.	Тема	Тема уведомления в письме для идентификации содержания.
2.	Текст	Текст уведомления в произвольном формате.
3.	Тип	Тип уведомления в зависимости от его важности.
4.	Отправить	Пользователи системы, которым централизованно отобразится сформированное уведомление.

После завершения ввода данных необходимо нажать кнопку «Отправить». При успешном выполнении всех действий отправленное сообщение должно отобразиться в таблице «История уведомлений». В дальнейшем для отправки похожего уведомления есть возможность восстановить параметры и текст ранее отправленного сообщения путем нажатия на иконку «Пересоздать» напротив соответствующего сообщения в функциональном разделе «История уведомлений».

Вложенная вкладка «События» содержит настройки выбора типов оповещения для администратора системы по выбранным каналам: Telegram, SMTP (Рисунок 60).

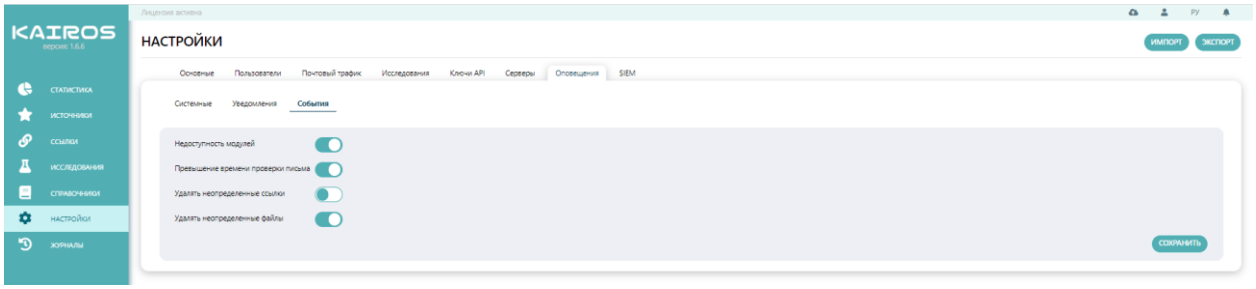

Рисунок 60. Вкладка «События»

Можно настроить оповещения о недоступности модулей в Системе, превышении лимита времени проверки письма, удалении неопределенных ссылок и файлов. По завершении ввода данных необходимо нажать кнопку «Сохранить».

Вкладка «SIEM» содержит настройки отправки событий системы в сервис SIEM (Рисунок 61).

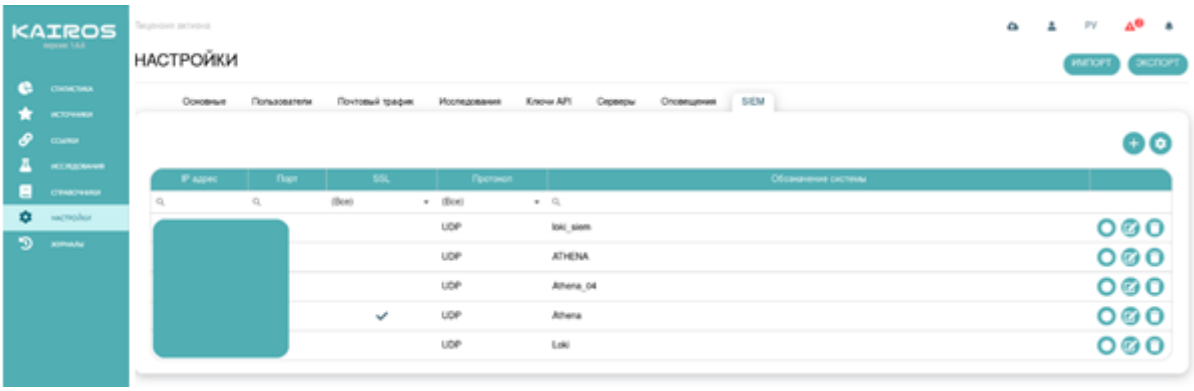

Рисунок 61. Настройки SIEM

В таблице перечислены все SIEM системы, с которыми интегрирована Система. Для внесения изменений в настройки отправляемых сообщений из Системы по протоколу Syslog во все SIEM системы следует нажать на кнопку «Общие настройки» в правом верхнем углу таблицы «SIEM» (Рисунок 62).

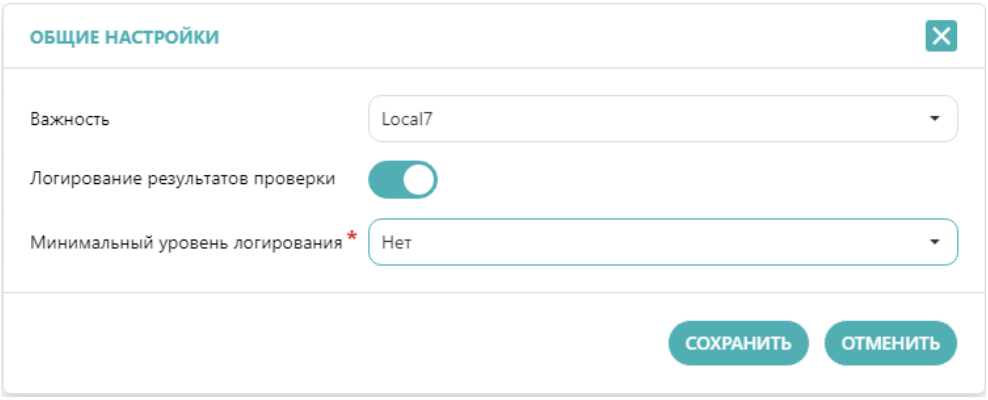

Рисунок 62. Общие настройки

В отобразившейся форме необходимо указать параметры, описанные в таблице 26.

Таблица 26. Общие настройки

№	Параметры	Описание
1.	Важность	Категория событий, передаваемых по протоколу Syslog в SIEM системы (Facility согласно RFC 5424 / RFC 3164).
2.	Логирование результатов проверки	Флаг, активирующий сбор данных в системном журнале по результатам проверки ссылок в Системе.
3.	Минимальный уровень логирования	В выпадающем меню выбирается уровень детализации информации по событиям системы, которая будет отправляться в SIEM.

По завершении ввода данных необходимо нажать кнопку «Сохранить».

Для подключения к новой SIEM системе следует нажать на кнопку «Добавить» в правом верхнем углу таблицы «SIEM» (Рисунок 63).

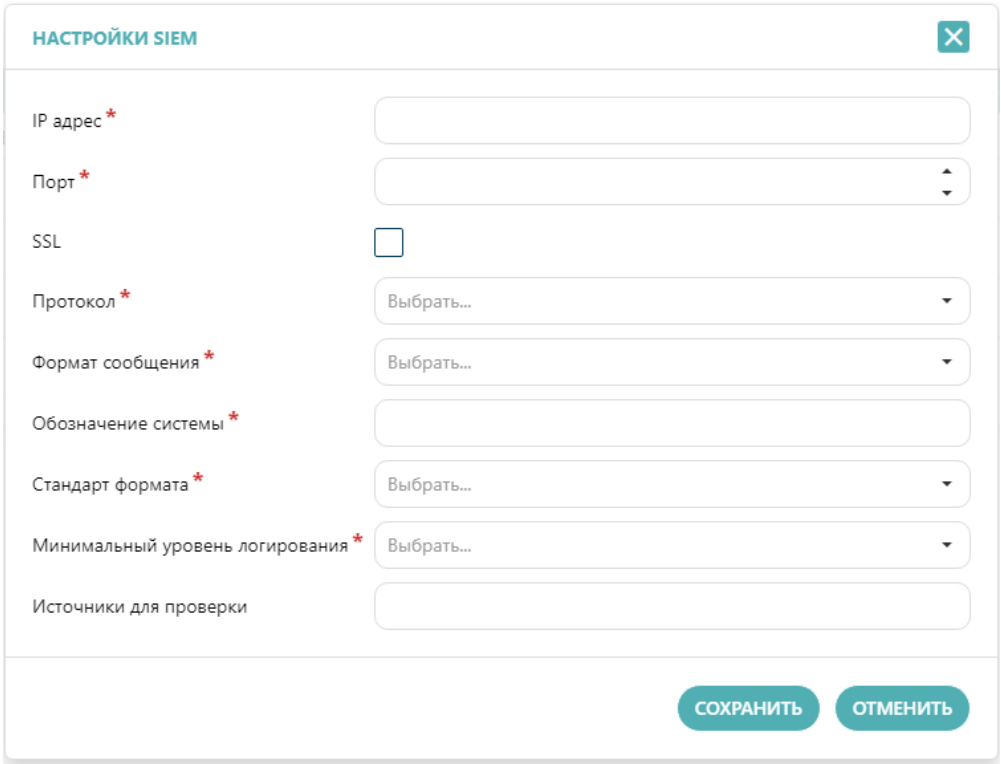

Рисунок 63. Добавление и настройка SIEM

В открывшейся форме следует заполнить параметры подключения к SIEM системе, исходя из их описания в таблице 27.

Таблица 27. Параметры подключения к SIEM

№	Параметры	Описание
1.	IP-адрес	IP-адрес системы SIEM.
2.	Порт	Открытый порт для взаимодействия с системой.
3.	SSL	Флаг, активирующий использование протокола шифрования SSL для повышения безопасности передачи данных в SIEM систему.
4.	Протокол	Выбор протокола передачи данных в систему.
5.	Формат сообщения	Выбор типа сообщений для передачи в SIEM.
6.	Обозначение системы	Идентификационное обозначение системы SIEM.
7.	Стандарт формата	Выбор формата сообщений системного журнала.

№	Параметры	Описание
8.	Минимальный уровень логирования	Выбор уровня важности отправляемых событий категории, выбранной в общих настройках (Рисунок 62), в систему SIEM.
9.	Источники проверки	В SIEM будут поступать события о ходе проверки ссылок, полученных только из указанных источников. События о ходе проверки ссылок из других источников в SIEM отправляться не будут.

После заполнения всех полей формы «Настройки SIEM» необходимо нажать на кнопку «Сохранить». Чтобы внести изменения в параметры подключения Системы к SIEM системе, необходимо воспользоваться иконкой «Редактировать» напротив нужной SIEM в таблице. Форма редактирования идентична форме добавления SIEM системы.

Если подключение к SIEM системе требует наличия сертификата у отправляющей стороны, сертификат можно загрузить через иконку «Настройки сертификата» напротив соответствующей SIEM системы (Рисунок 64).

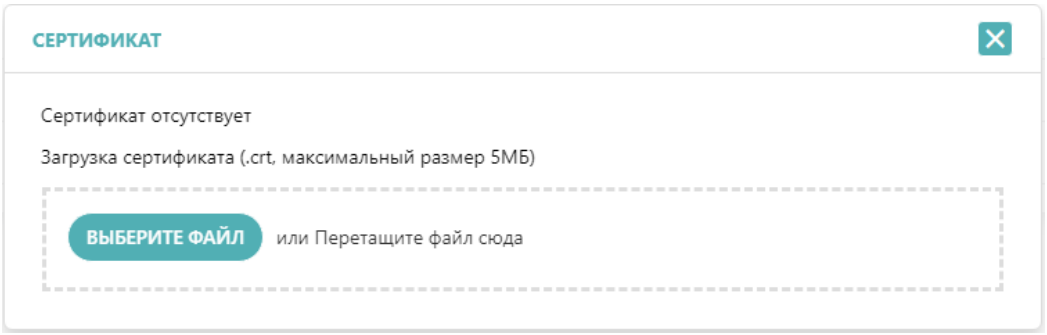

Рисунок 64. Добавление сертификата SIEM

6 Журналы

В разделе «Журналы» присутствуют данные мониторинга значимых действий, процессов и ресурсов системы (Рисунок 65).

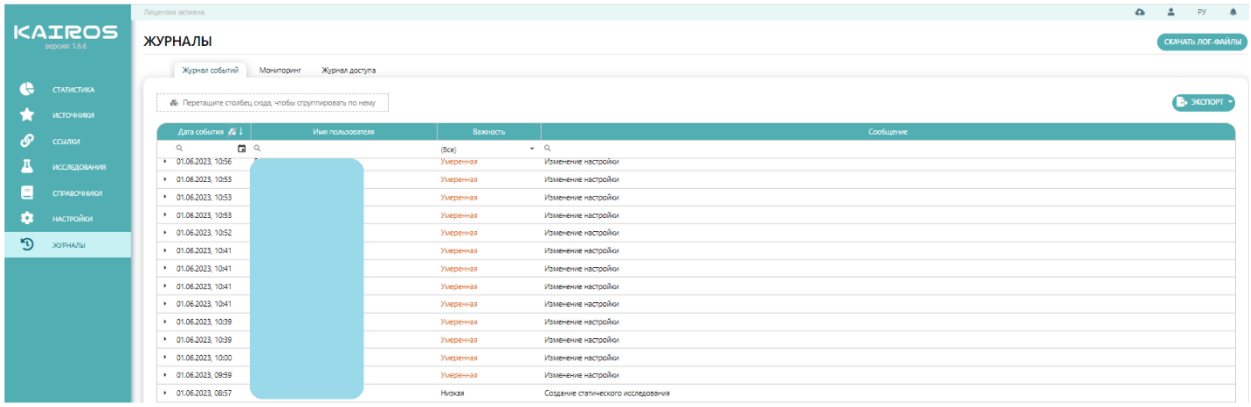

Рисунок 65. Раздел «Журналы»

Назначения журналов в системе описаны в таблице 28.

Таблица 28. Назначение системных журналов

№	Наименование журнала	Назначение
1.	Журнал событий	Фиксирует значимые действия пользователей в системе.
2.	Мониторинг	Фиксирует использование физических ресурсов системы.
3.	Журнал доступа	Фиксирует авторизацию в системе пользователей и подключения по API.

Во вкладке «Журнал событий» регистрируются действия пользователей, по каждому действию можно посмотреть более подробную информацию, нажав на раскрывающий элемент. Система предоставляет по каждой записи следующую информацию:

– Дата, время действия пользователя

– Имя пользователя в системе

– Важность действия (низкая, средняя, высокая)

– Описание действия пользователя

Во вкладке «Мониторинг» отображается использование физических ресурсов системой (Рисунок 66).

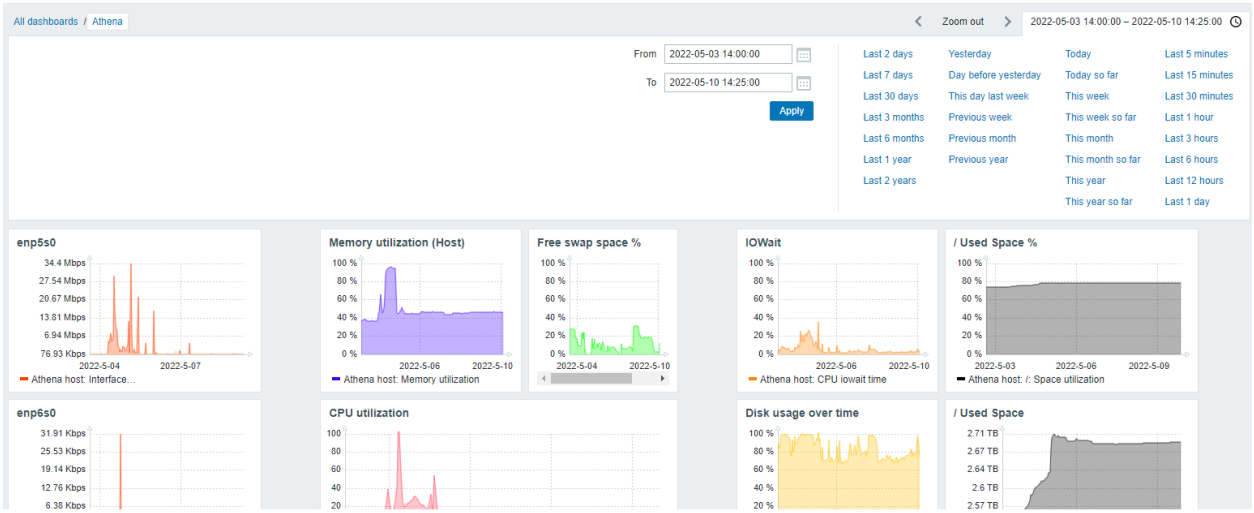

Рисунок 66. Мониторинг использования физических ресурсов системой

Во вкладке «Журнал доступа» присутствует информация по журналированию авторизации пользователей и модулей в системе, так же подключение API (Рисунок 67 - 68).

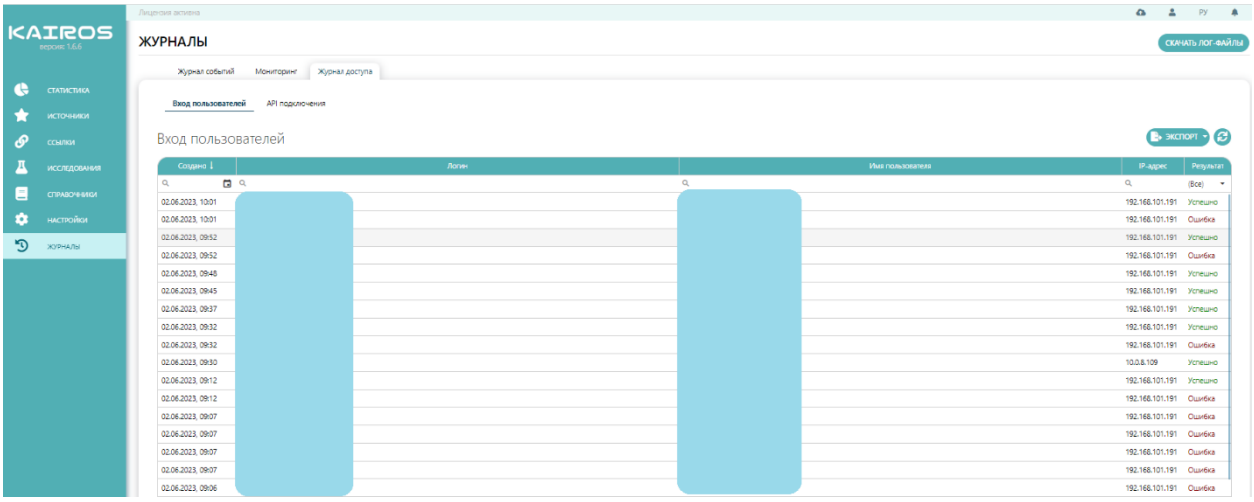

Рисунок 67. Журнал доступа в систему

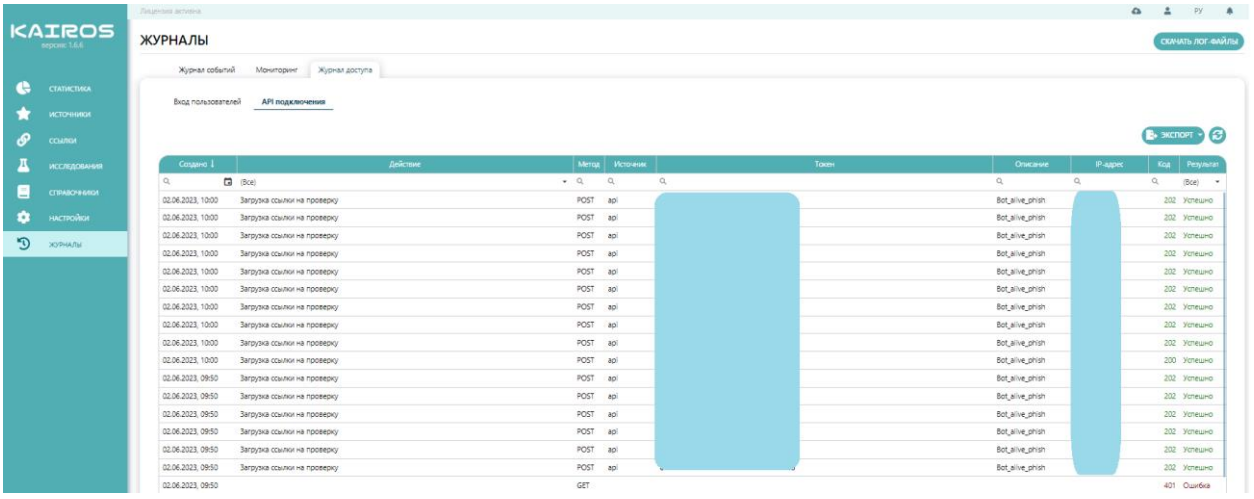

Рисунок 68. Журнал подключений API

7 Решение возможных проблем

При проверке почтового трафика могут возникнуть следующие типы нештатных ситуаций, которые описаны в таблице 29.

Таблица 29. Описание решения нештатных ситуаций

№	Проблема	Описание решения
1.	Система недоступна	Перенаправление трафика обратно на внутренний почтовый сервер.
2.	Ложное срабатывание системы	Извлечение семпла в запароленом архиве согласно РП по Системе и отправка на перепроверку в открытые схожие по функционалу классы систем антивирусного мультисканера и песочницы: https://app.any.run/ https://www.virustotal.com/gui/home/upload Если результаты сходятся с Системой, но есть подозрение, что это ложное срабатывание, то просьба связаться со службой поддержки АВ Софт по электронной почте support@avsw.ru и по телефону +7 (495) 988-92-25.
3.	DNS сервер не отвечает или недоступен	Перепроверить работу маршрутизатора Перепроверить работу провайдера Проверить доступность DNS с MTA Системы следующими типами команд: – nslookup – ping – traceroute – nc – curl – dig

№	Проблема	Описание решения
		Проверить состояние службы на DNS сервере, если имеется доступ следующими типами команд: – nslookup – ping – traceroute – nc – curl – dig
4.	Блокировка SMTP и DNS трафика межсетевым экраном	Перепроверить настройку политик на предмет блокировки отправки трафика на хост сервера с MTA Системы.
5.	Перестали приходить письма	Убедитесь, что настройки DNS и MX записи почтового сервера действительно направляют почтовый трафик на домен Системы.
6.	Закрылся почтовый порт	Проверить открытыли почтовые порты: SMTP – 25/tcp SMTP (стандартный порт) – 465/tcp SMTPS (устаревший) – 587/tcp submission (порт для обслуживания клиентов) POP3 – 110/tcp POP3 (стандартный порт) – 995/tcp POP3S (порт с предварительной установкой SSL/TLS соединения) IMAP – 143/tcp IMAP (стандартный порт)

№	Проблема	Описание решения
		– 993/tcp IMAPS (порт с предварительной установкой SSL/TLS соединения) Проверку можно выполнить следующими способами: – Netstat sudo netstat -ltup – Команда ss sudo ss -lntu – Утилита Nmap sudo nmap -n -PN -sT -sU -p- localhost – Утилита lsof sudo lsof -i
7.	Отсутствует соединение между MTA системы ATHENA до почтового сервера заказчика	Проверить правильность маршрутизации при помощи службы traceroute Проверить настройки маршрутизатора и межсетевого экрана
8.	Получение копий одного и того же письма	Письма могут приходить повторно - это может быть связано с неполучением подтверждения того, что письмо уже было доставлено, где-то в процессе доставки электронной почты. Так как оригинальная копия была поставлена в очередь на локальную доставку, она дойдет, но поскольку сервер-отправитель так и не получил подтверждения, то он попытается доставить сообщение еще раз, что приведет к появлению дубликатов писем. Это более вероятно, когда сервер или Система находятся под большой нагрузкой, или

№	Проблема	Описание решения
		когда сообщение передается по сети с высокой задержкой. Это временная проблема, и обычно доставляется только одно письмо. Повторные копии можно удалить.
9.	Загрузка всех входящий сообщений через MUA после обслуживания почтового сервера.	Скорее всего ваш MUA использует протокол POP3 для соединения с сервером, и это соединение было сброшено, письма остались на сервере, а не были загружены. Чтобы этого не происходило в будущем, вы можете либо настроить MUA на удаление сообщений с сервера через определенный период времени, либо перейти на использование протокола IMAP вместо POP3. IMAP всегда синхронизируется с сервером, поэтому опасность повторной загрузки сообщений отсутствует.

8 Команды Shell

Для доступа к интерпретатору командной строки необходимо выполнить авторизацию в соответствии с учетными данными, выданными ранее вендором системы KAIROS.

AVSoft Shell имеет следующий общий список команд, описанный в таблице 30.

Таблица 30. Описание команд

№	Команда	Описание	Использование
1.	apt	Настройка APT proxy	apt COMMAND [http|https] [url] COMMAND: edit – редактирование прокси del – удаление прокси info – информация о прокси

№	Команда	Описание	Использование
2.	change_password	Изменяет пароль пользователя avsoft_shell на указанный в команде	change_password [password] password — новый пароль

3.	check_port	Проверка доступности удалённого порта	check_port [Protocol] [address] [port]
			Protocol:
			-t - Протокол TCP (По умолчанию)
			-u - Протокол UDP
			Пример:
			$ check_port 192.168.10.101 22
			Connection to 192.168.10.101 22 port [tcp/sshd] succeeded!
			$ check_port -u 192.168.10.102 514

4.	clear	Очистка терминала от текста	clear
5.	hostname	Устанавливает имя хоста.	hostname [HOSTNAME] HOSTNAME: Имя хоста, может состоять из букв латинского алфавита, цифр и дефиса.

AVSoft Shell для кластера InfraCluster имеет следующий список команд, описанный в таблице 31.

Таблица 31. Описание команд для кластера

№	Команда	Описание	Использование
1.	prepare_node	Подготавливает ноду для работы в кластере, запускает сервис singletoner.	prepare_node
2.	cluster_node	Программа для добавления ноды в кластер.	cluster_node --node_type [NODE_TYPE] --ip [IP_ADDRESS1] --ip [IP_ADDRESS2] --module [MODULE] --role [ROLE] Аргументы: --node_type — тип ноды, infra или nginx. --ip — IP-адрес, можно указать несколько раз для нескольких IP-адресов. --module — название модуля, на текущий момент доступен только kairos. --role — роль ноды, primary или slave
3.	prepare_slave	Удаляет существующие директории с данными БД.	prepare_slave
4.	vip	Работа с виртуальными IP-адресами, настройка keepaliverd.	vip add|del add — добавляет виртуальный IP-адрес кластера del — удаляет виртуальный IP-адрес кластера

№	Команда	Описание	Использование
			Использование vip add: vip add --ip <IP-адрес кластера> --weight <вес> --u_peer <IP-адрес второй ноды> --ip — IP-адрес, по которому будет доступен Kairos --weight — приоритет ноды в кластере, числовое значение от 0 до 255 --u_peer — IP-адрес второй ноды в кластере На второй ноде в кластере необходимо в параметре --u_peer указать IP-адрес первой ноды: vip add --ip <IP-адрес кластера> --weight <вес> --u_peer <IP-адрес первой ноды>

AVSoft Shell имеет следующий список команд для сетевого интерфейса, описанный в таблице 32.

Таблица 32. Описание команд для сетевого интерфейса

№	Команда	Описание	Использование
1.	interface [add|edit|info|primary]	Работа с сетевыми интерфейсами.	interface [add|edit] [INTERFACE] [TYPE] interface [add|edit] [INTERFACE] [TYPE] [--ip IPV4] [--nm NETMASK] [--gw GATEWAY] TYPE:

№	Команда	Описание	Использование
			dynamic — для настройки динамических парамтеров сети. static — для настройки статических параметров сети. Опциональные аргументы: -h, --help отобразить данное сообщение и выйти --ip IPV4 IPv4 адрес интерфеса --nm NETMASK Маска подсети --gw GATEWAY Шлюз по-умолчанию
2.	interface primary	Установка интерфейса основным.	interface primary [INTERFACE]
3.	interface up|down	Включение/выключение интерфейса.	interface up|down [INTERFACE] interface route [INTERFACE] [COMMAND]... Работа со статическими маршрутами. COMMAND:

№	Команда	Описание	Использование
			info — информация о маршрутах. add — добавить статический маршрут (подробности по команде ниже). del — удалить статический маршрут (подробности по команде ниже).
4.	interface route [INTERFACE] add	Добавление статического маршрута.	interface route [INTERFACE] add --ip [IPV4] --nm [NETMASK] --gw [GATEWAY] Опциональные аргументы: -h, --help отобразить данное сообщение и выйти --ip IPV4 IPv4 адрес --nm NETMASK Маска подсети --gw GATEWAY Шлюз
5.	interface route [INTERFACE] del	Удаление статического маршрута.	interface route [INTERFACE] del [IDX]

№	Команда	Описание	Использование
			Опциональные аргументы: -h, --help отобразить данное сообщение и выйти IDX — индекс статического маршрута
6.	logs	Вывод информации из логов.	logs syslog
7.	nginx	Управление nginx.	nginx [COMMAND] COMMAND: enable — переносит сервис (сайт) nginx в секцию активных. disable — удаляет сервис (сайт) nginx из секции активных. show — отобразить все активные и доступные сервисы (сайты) nginx. test — тестирование конфигурационного файла. reload — перезагрузка конфигурации, старт нового рабочего процесса с новой конфигурацией
8.	nmcli	Предоставляет доступ к UNIX-утилите nmcli.	nmcli [OPTIONS] [SECTION] [ACTION]

№	Команда	Описание	Использование
9.	network_restart	Перезапуск службы network-manager.	network_restart
10.	ntp	Установка NTP-серверов, синхронизация времени с установленным NTP-сервером	ntp [NTP1_IP NTP2_IP … NTPN_IP]
11.	ping	Предоставляет доступ к утилите ping.	ping [OPTIONS] DESTINATION_IP DESTINATION_IP — IP-адрес для теста.
12.	scp	Отправка логов целевому устройству.	scp logs [TARGET] TARGET - цель для отправки логов Пример: scp logs user@192.168.0.5:~/data
13.	settings	Просмотр и редактирование конфигурационного файла config.json.	settings [COMMAND] [MODULE] [KEYNAME] [VALUE] COMMAND: info - информация о текущих настройках change - изменить настройку в модуле MODULE, ключе KEYNAME, установить значение VALUE.

№	Команда	Описание	Использование
14.	shutdown	Выключение устройства.	shutdown -y
15.	reboot	Выключение устройства.	reboot -y
16.	traceroute	Предоставляет доступ к консольной утилите traceroute.	traceroute [OPTIONS] host [PATHLENGTH]
17.	type	Изменение типа консоли AVSoft Shell.	type info|set [TYPE] TYPE: Тип консоли может быть одним из следующих: signature, balancer, sensor_deception, loki

8.1 Обновление через репозиторий

Обновление выполняется следующей последовательностью команд:

```
apt update
apt install -y apt list --upgradeable | grep ^mailcheck- | sed 's;/.*;;g'
apt install -y apt list --upgradeable | grep ^core-linkcheck | sed 's;/.*;;g'
apt install kairos-web


apt-get install --reinstall kairos-web
```