AVSOFT KAIROS v2

Система защиты от спама и фишинга

Руководство пользователя

Москва
2024 г

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 пользователя v2.4

Апрель 5, 2024

Релиз 1.7.5

СОДЕРЖАНИЕ

1 Термины и определения

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

Таблица 1. Термины и определения

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

2 Перечень сокращений

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

Таблица 2. Перечень сокращений

№	Сокращение	Значение
1.	API	Application Programming Interface
2.	CPU	Central Processing Unit
3.	DKIM	DomainKeys Identified Mail
4.	DMARC	Domain-based Message Authentication, Reporting and Conformance
5.	DNS	Domain Name System
6.	ID	Identifier
7.	HTTP	Hypertext Transfer Protocol
8.	HTTPS	Hypertext Transfer Protocol Secure
9.	ML	Machine Learning
10.	SPF	Sender Policy Framework
11.	ВПО	Вредоносное программное обеспечение
12.	ОС	Операционная система
13.	ПО	Программное обеспечение

3 Назначение программы

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 и вредоносных вложений

Система анализирует все письма, поступающие на почтовые сервера. Письма проходят проверку в двух функциональных разделах системы:

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

Проверка писем на спам проводится за счет анализа его текста и технических заголовков. В проверке участвуют модули SPF, DKIM, DMARC, Spam Score, ML. Также разделом машинного обучения осуществляется определение категории контента письма (например, рассылка, деньги, разработка ПО, переписка).

Проверка писем на фишинг проводится за счет анализа ссылок в письме и технических заголовков. В проверке участвуют модули ML, внешние аналитические ресурсы XSEO, PhishTank, UrlScan, VirusTotal и индикаторы заголовков.

Проверка вложений включает в себя анализ одним антивирусным движком. (Если присутствует интеграция с системой AVSOFT ATHENA, то все вложения отправляются в нее на проверку без проверки антивирусом в AVSOFT KAIROS v2. После завершения проверки AVSOFT ATHENA результаты отображаются в AVSOFT KAIROS v2).

Результатом проверки письма является его вердикт. Система присваивает письму один из трех вердиктов:

- Безопасный
- Подозрительный
- Вредоносный.

Каждый из вердиктов имеет свою цветовую индикацию. Подозрительный и вредоносный вердикты относятся к небезопасным вердиктам. Система политик позволяет гибко настроить политики доставки и блокировки писем получателям с определенным вердиктом, а также сделать фильтрацию по проверке или исключению из нее от определенных источников.

По умолчанию в Системе настроен режим оптимизации проверки, по котороме письма, не прошедшие проверку на спам, блокируются системой и не проверяются остальными инструментами анализа

Если письмо по результатам проверки на спам в первом разделе получает безопасный вердикт и содержит ссылки на веб-ресурсы или вложения, оно направляется на проверку во второй раздел. При отсутствии ссылок или вложений, письмо также отправляется на анализ почтовых заголовков во второй раздел.

После проверки гибкая система настроек позволяет выборочно вырезать вредоносные или подозрительные объекты из письма при доставке получателю.

4 Авторизация и элементы управления

4.1 Авторизация в Системе

Для авторизации в Системе необходимо ввести логин и пароль, полученный у администратора (Рисунок 1).

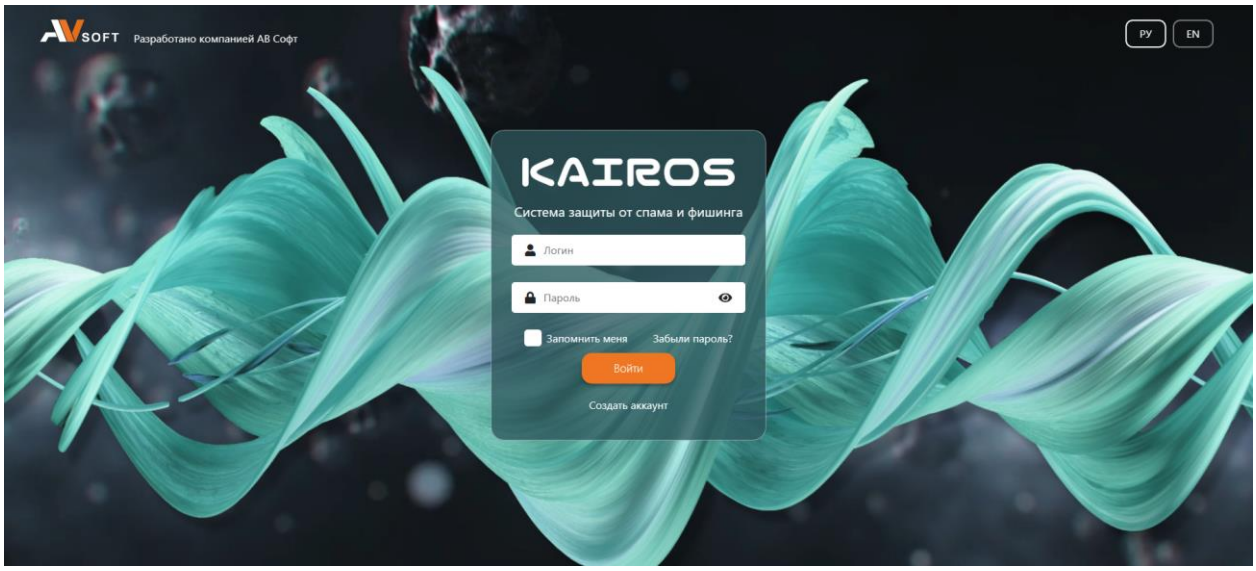

Рисунок 1. Страница авторизации пользователя в системе KAIROS

В Системе доступна двухфакторная. Для этого нужно:

1. Скачать специализированное приложение на телефон (например, Яндекс Ключ или Google Authenticator).
2. В профиле пользователя включить флаг * ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ.
3. Сканировать QR код (появляется при включении флага) и приложение начнет генерировать временные ключи (Рисунок 2).

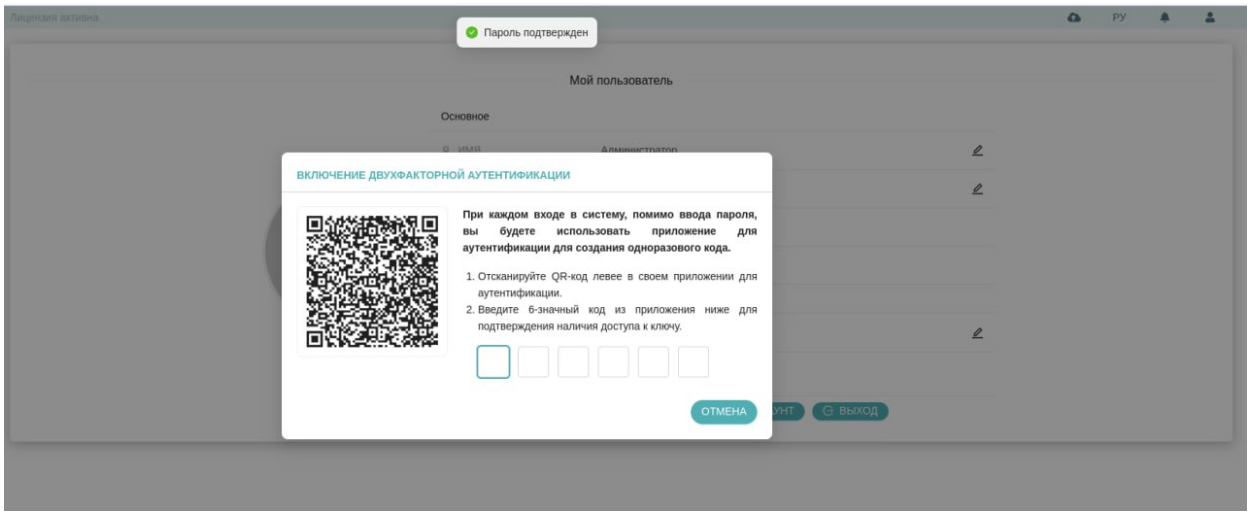

Рисунок 2. Пример сгенерированного QR-кода

4. При авторизации в KAIROS нужно ввести полученный ключ (после ввода логина и пароля).

После прохождения авторизации осуществляется переход в веб-интерфейс Системы KAIROS v2, в котором присутствуют функциональные разделы, описанные в таблице 3.

Таблица 3. Описание функциональных разделов в системе

№	Раздел	Описание
1.	Статистика	Содержит статистическую информацию
2.	Почтовый трафик	Содержит информацию по всем письмам, поступающим в систему, по SMTP-сессиям и по серому списку
3.	Ссылки	Содержит информацию по всем веб-ссылкам, исследованным в системе
4.	Политики	Содержит информацию по первичной проверке, профилям, политикам и группам в системе
5.	Справочники	Содержит шаблоны регулярных выражений, белый и черный списки, а также перечень индикаторов почтовых заголовков, использующихся в системе
6.	Настройки	Содержит настройки по всем компонентам системы

№	Раздел	Описание
7.	Журналы	Содержит информацию по мониторингу всех логических и физических модулей в системе, а также регистрацию действий пользователей

4.2 Элементы управления веб-интерфейсом

Описание, назначение и настройки по умолчанию элементов управления веб-интерфейсом Системы представлены в таблице 4.

Таблица 4. Элементы управления интерфейсом

№	Элемент	Назначение	Изображение
1.	Кнопка «Загрузка файлов»	Выполняет загрузку файла на проверку	
2.	Кнопка «Учётная запись»	Выполняет переход в меню личного кабинета	
3.	Кнопка «Язык»	Позволяет выбрать язык отображения интерфейса	
4.	Кнопка «Неактивные модули»	Появляется при уведомлениях системы	
5.	Кнопка «Уведомления»	Позволяет увидеть уведомления, которые выдает система	
6.	Кнопка «Обновить»	Обновления данных в таблице	
7.	Кнопка «Отправить выделенные письма»	Повторная отправка адресату выбранных писем	
8.	Кнопка «Печать»	Формирование печатного отчета	

№	Элемент	Назначение	Изображение
9.	Кнопка «Выбор столбцов»	Выбор столбцов для отображения в таблице	
10.	Кнопка «Копировать»	Выполняет копирование	
11.	Кнопка «Отчет»	Отображение отчета по результатам проверки объекта	
12.	Кнопка «Изменить вердикт»	Выполняет редактирование вердикта ссылки	
13.	Кнопка «Редактировать»	Выполняет редактирование информации	
14.	Кнопка «Машинное обучение»	Отображает результат анализа ссылки моделями машинного обучения	
15.	Кнопка «Добавить»	Выполняет добавление нового объекта	
16.	Кнопка «Удалить»	Осуществляет удаление выбранной записи	
17.	Кнопка «Редактировать группы пользователей»	Отображает форму для редактирования группы пользователей	
18.	Кнопка «Боты»	Отображает окно с данными об обработчиках данных ботов	

№	Элемент	Назначение	Изображение
19.	Кнопка «Журнал работоспособности»	Отображает информацию о проверках модулей	
20.	Кнопка «Графики»	Отображает собранную статистику по работе ботов	
21.	Кнопка «Настройки»	Отображает форму для изменения настроек	
22.	Кнопка «Остановить»	При нажатии на кнопку будет осуществлена остановка объекта, например, бота	
23.	Кнопка «Запустить»	При нажатии на кнопку будет осуществлён запуск объекта, например, бота	
24.	Кнопка «Настройка сертификата»	Отображает форму для загрузки сертификата	

Элементы управления веб-интерфейсом имеют всплывающие подсказки, которые отображают их названия.

4.3 Требования к браузерам

В таблице 5 представлены минимальные требования к версиям браузера (веб-обозревателя), необходимые для функционирования веб-интерфейса Системы.

Таблица 5. Минимальные версии браузера

№	Браузер	Версия браузера
1.	Chrome	80
2.	Edge	80
3.	Firefox	74
4.	Opera	67

5 Раздел «Статистика»

В разделе «Статистика» во вкладке «Аналитика» - «Ссылки» представлены диаграммы со статистическими данными по вердиктам проанализированных ссылок, источникам, доменов их поступления в систему, а также графики по вердиктам проверок. Во вкладке «Вредоносные ссылки» можно посмотреть отчет о проверке ссылки, нажав на иконку «Отчет» (Рисунок 3).

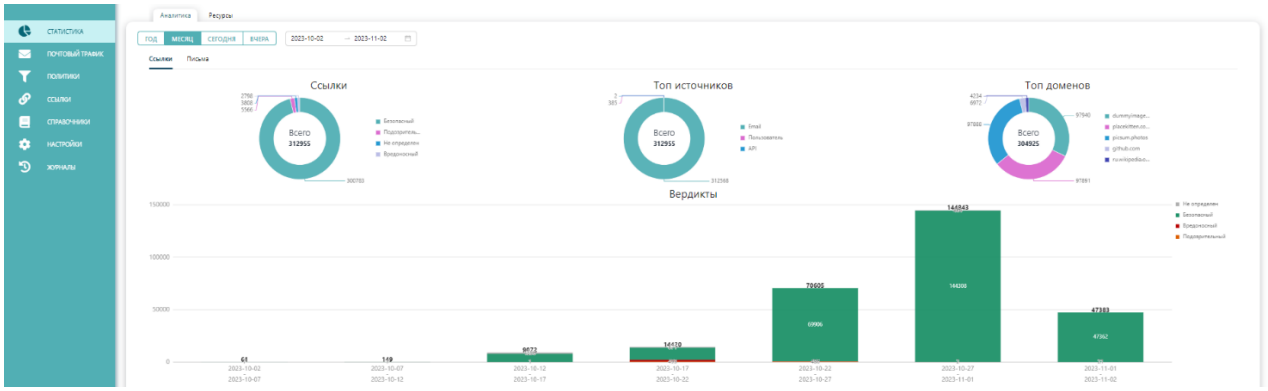

Рисунок 3. Раздел «Статистика», вкладка «Аналитика» - «Ссылки»

При нажатии на вкладку «Письма» осуществляется переход в раздел писем, в котором можно посмотреть круговые диаграммы, в которых отражаются проверки, блокировки и ошибки, а также отчеты по вредоносным письмам, нажав иконку «Отчет» (Рисунок 4).

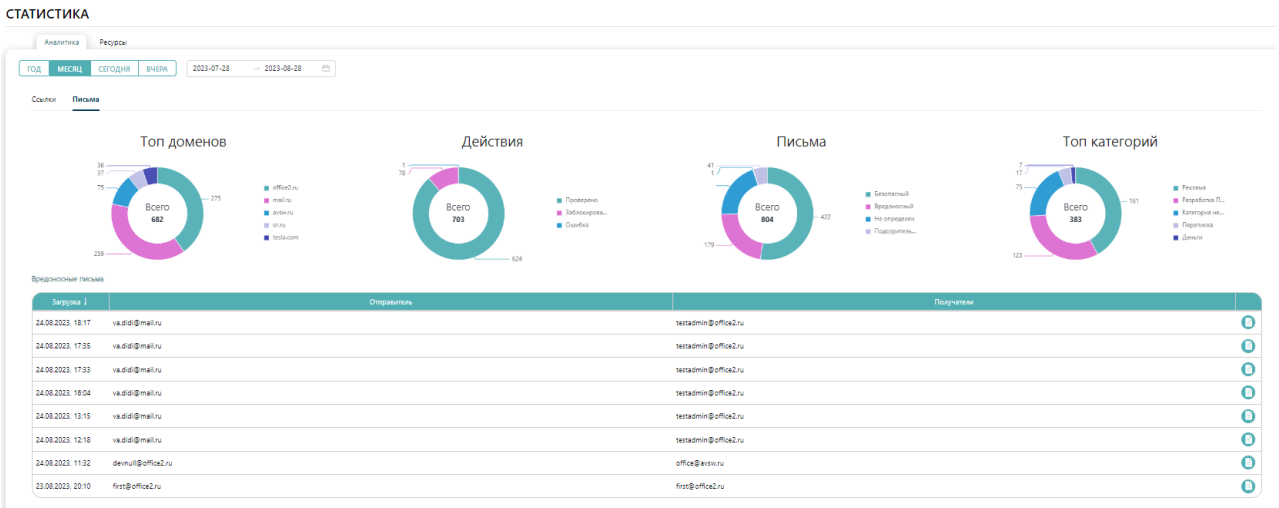

Рисунок 4. Активная кнопка «Письма»

Во вкладке «Ресурсы» находятся графики состояния производительности и загруженности модулей обработки писем на спам и анализа на фишинг (выводятся данные о свободном и занятом месте, ошибках и вердиктах) (Рисунок 5).

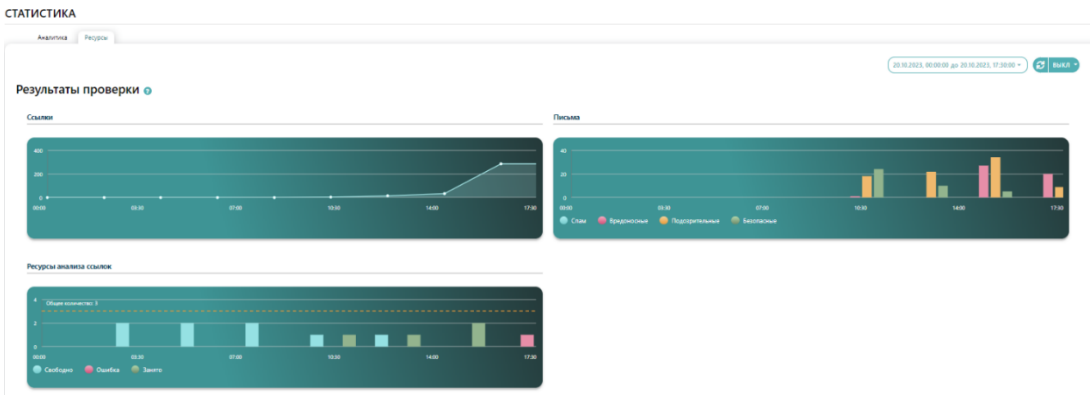

Рисунок 5. Раздел «Статистика» вкладка «Ресурсы»

При нажатии на «Справку» рядом с наименованием графика, будет отображено подробное описание раздела.

Также есть возможность настроить временной интервал для отображения графиков (Рисунок 6).

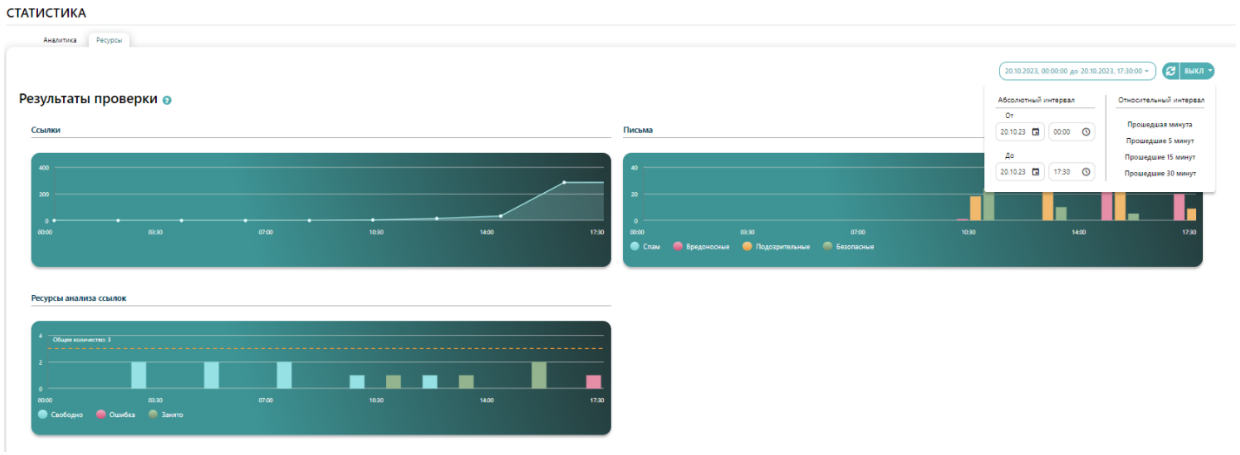

Рисунок 6. Настройка временного интервала

Элементы на графиках являются активными, при нажатии на них происходит автоматическая фильтрация по выбранной категории. Для указания периода времени, за который требуются статистические данные, необходимо воспользоваться пейджером над схемами.

6 Раздел «Почтовый трафик»

В разделе «Почтовый трафик» содержится информация по всем письмам, поступающим в Систему и результаты их проверки, информация по SMTP-сессиях и по серому списку (Рисунок 7).

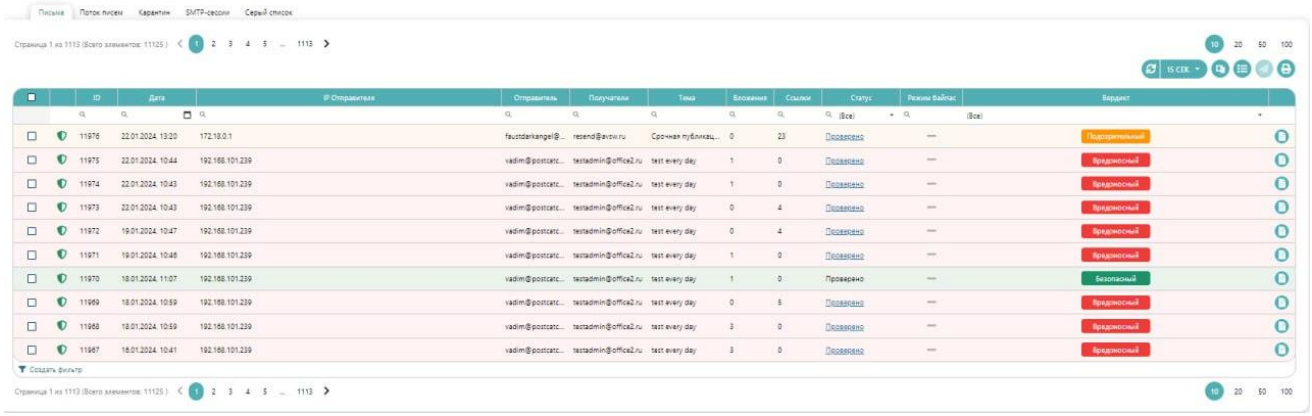

Рисунок 7. Раздел «Почтовый трафик»

Информацию о всех получателях можно посмотреть в колонке «Получатели». При наличии у одного письма нескольких получателей, в отчете письма будут написаны адреса всех получателей, как и в графе письма. Колонка «Режим байпас» отображает статус данного режима. Также здесь отображается поток писем, которые система приняла на проверку. Результаты попытки установки сессии передачи данных находятся во вкладке «SMTP сессии». Почтовые сервера, предположительно отправившие спам, отображаются во вкладке «Серый список».

Во вкладке «Поток писем» отображается информация о потоке писем, которые поступают на систему (Рисунок 8)

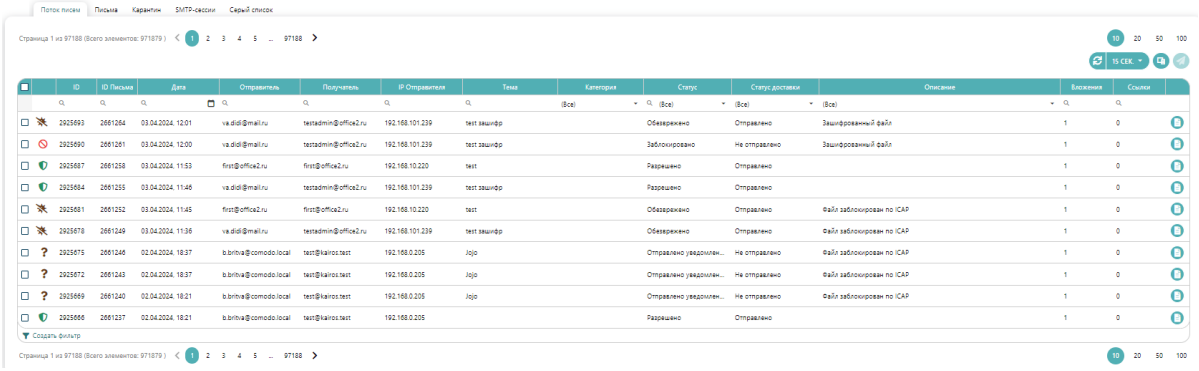

Рисунок 8. Поток писем

По каждому из писем имеется отчет, в котором отображается информация, показывающая статусы проверки письма в системе (Рисунок 9)

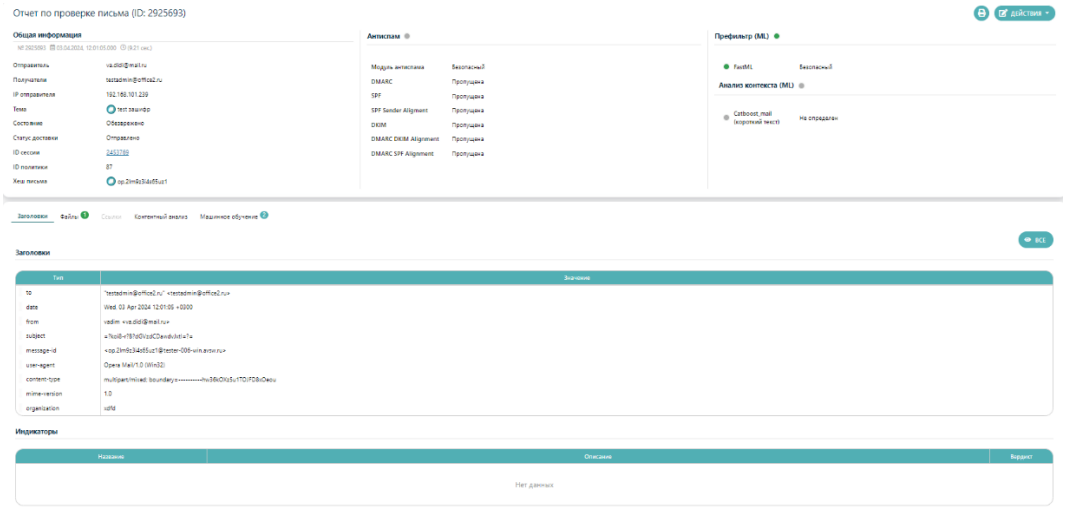

Рисунок 9. Отчет по письму

6.1 Серый список

Во вкладке «Серый список» отображаются адреса почтовых серверов, который после отправки первого запроса в Систему получили отрицательный ответ и не возобновили попытку установки сессии снова. (Рисунок 10).

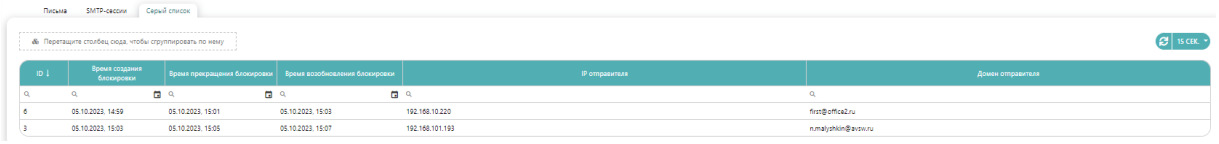

Рисунок 10. Вкладка «Серый список»

Данные, представленные в таблице, отражены в таблице 6.

Таблица 6. Данные таблицы «Серый список»

№	Параметры	Описание
1.	Время создания блокировки	Первый запрос
2.	Прекращение блокировки	После этого времени все письма пользователя не будут подвергаться грей листинг
3.	Время возобновления	После этого времени грей листинг начнёт опять работать по IP-адресу и домену, если превышено время, заданное в Настройках «Почтовый трафик» -> «Основное» -> «Серый список» с момента первого запроса

6.2 Отчет по проверке письма

Обоснованием вердикта письма является отчет по его проверке. Просмотреть отчет можно в разделе «Почтовый трафик» - «Письма», нажав на иконку «Отчет». Уникальным идентификатором отчета является его ID (Рисунок 11).

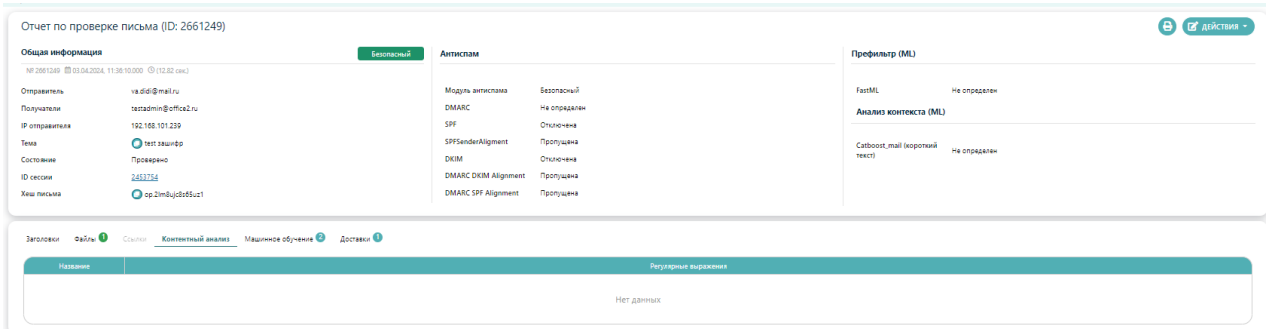

Рисунок 11. Отчет по проверке письма

Отчет состоит из следующих основных разделов:

– Раздел проверки письма

– Результат анализа артефактов письма

Раздел проверки письма содержит следующую информацию:

– Общая информация

– Антиспам

– Префильтр (ML)

– Анализ контекста (ML)

Раздел анализа артефактов письма содержит следующую информацию:

– Метаданные почтовых заголовков

– Файлы (вложения письма)

– Ссылки (содержащиеся в письме)

– Контентный анализ

– Машинное обучение

– Доставки

В разделе «Общая информация» содержатся данные, перечисленные в таблице 7.

Таблица 7. Общая информация

Поле	Информация
Вердикт	Вердикт, присвоенный письму по результату проверки
Отправитель	Почта отправителя письма
Получатели	Почта получателя (получателей) письма
IP отправителя	IP-адрес отправителя письма
Тема	Тема письма
Статус доставки	Статус по доставке письма в системе
ID сессии	Указание номера идентификатора сессии
ID письма	Указание номера идентификатора письма

В разделе имеется возможность проводить различные действия с отчетом. Для этого нужно зайти во вкладку «Отчет», нажать кнопку «Действия» и выбрать нужное действие (Рисунок 12)

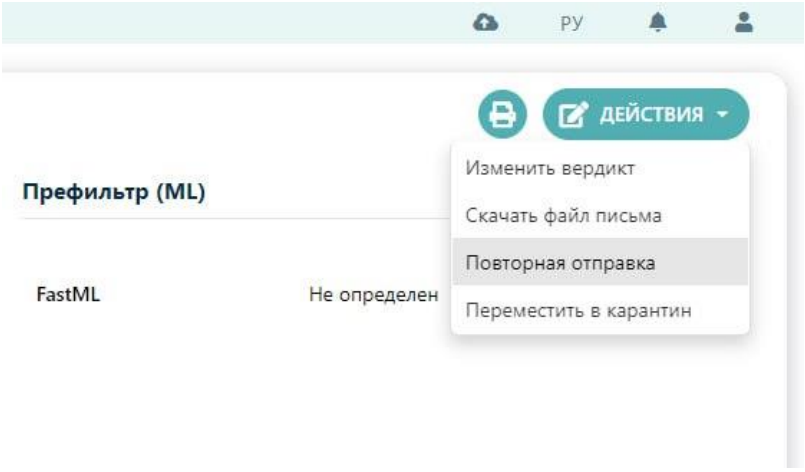

Рисунок 12. Действия с отчетом

При формировании печатного отчета нужно выбрать действие «Печать» и после этого будет сформирован печатный отчет в формате pdf (Рисунок 13, Рисунок 14).

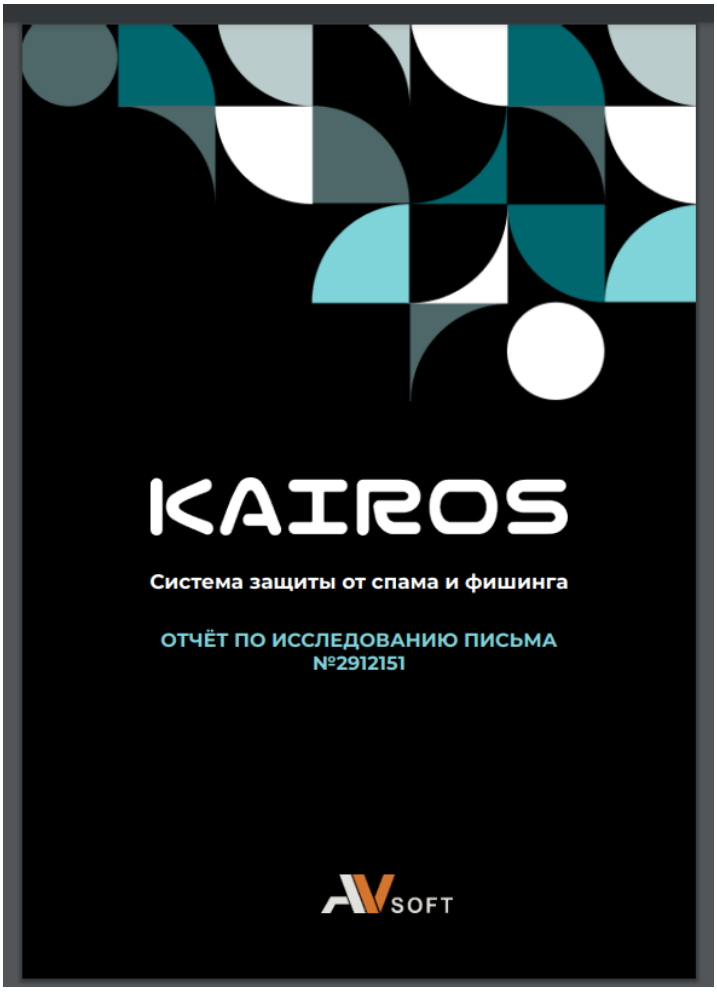

Рисунок 13. Обложка печатного отчета

Рисунок 14. Содержание печатного отчета

6.3 Проверка письма на спам

Раздел отчета «Антиспам» содержит результаты проверки письма на спам, сформированные различными модулями и политиками проверки: DKIM, DMARC, SPF, Модуль антиспама. Технология анализа письма на спам данными модулями описана в таблице 8.

Таблица 8. Политики проверки письма на спам

Политика	Технология анализа	Результат анализа	Формируемый вердикт
DKIM	DKIM отмечает исходящую почту зашифрованной подписью внутри заголовка, а почтовый сервер получателя расшифровывает ее, используя открытый ключ шифрования, чтобы убедиться, что сообщение не было изменено при пересылке. В результате проверки цифровой подписи DKIM формирует почтовый заголовок.	Pass	безопасный
		None	
		Fail	вредоносный
		Policy	
		Neutral	
		TempError	
		PermError	
DMARC	DMARC проверяет репутацию почтовых сервисов и интернет-провайдеров. Технология DMARC требует, чтобы домен, используемый для передачи результата DKIM или SPF совпадал с доменом заголовка “From” в теле письма.	Pass	безопасный
		Fail	вредоносный
SPF	SPF подтверждает, что сообщения с конкретного	Pass	безопасный
		None	

Политика	Технология анализа	Результат анализа	Формируемый вердикт
	домена были отправлены с сервера, который контролируется владельцем этого домена. В результате проверки цифровой подписи SPF формирует почтовый заголовок.	Fail	вредоносный
		SoftFail	
		Neutral	
		TempError	
		PermError	
Spam Ignore	Spam Ignore обнаруживает спам различными методами, в т.ч. при помощи черных списков DNS, нечеткой контрольной суммы, байесовской фильтрации, внешних БД шаблонов спама. Spam Ignore анализирует тело и заголовок сообщения, выставляя оценку каждому проверяемому параметру на принадлежность к спаму. Итоговая оценка состоит из суммы всех оценок параметров.	Менее 5.0	безопасный
		Равно и более 5.0	вредоносный
Модуль антиспама	Объединяет результаты анализа двух технологий: Spam Ignore и ML	Spam Ignore безопасный + ML безопасный	безопасный
		Spam Ignore безопасный + ML подозрительный	подозрительный

Политика	Технология анализа	Результат анализа	Формируемый вердикт
		Spam Ignore безопасный + ML вредоносный	вредоносный
		Spam Ignore вредоносный + ML безопасный	
		Spam Ignore вредоносный + ML подозрительный	
		Spam Ignore вредоносный + ML вредоносный	

Так же раздел проверки на спам содержит результат анализа письма модулями машинного обучениями и имеет два раздела:

– Префильтр (ML),

Префильтр — это быстрая нейронная сеть, которая отсекает явный спам на большом потоке писем.

Во вкладке «Заголовки» отображаются метаданные почтовых заголовков и результат их анализа индикаторами заголовков Системы. Каждый из индикаторов направлен на проверку определенного почтового заголовка. При обнаружении подозрительных или вредоносных данных в заголовке письма, в разделе «Заголовки» отчета отображается сработавший индикатор и его описание (Рисунок 15).

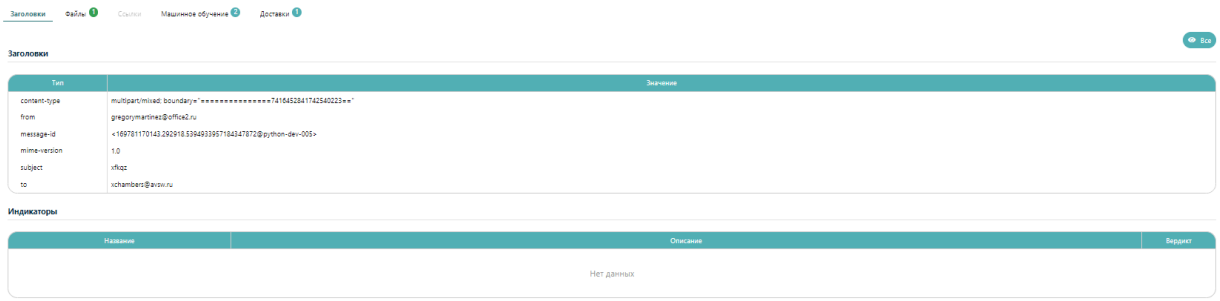

Рисунок 15. Отчет по проверке письма, вкладка «Заголовки»

Перечень почтовых заголовков, проходящих проверку в Системе индикаторами заголовков, представлен в таблице 9.

Таблица 9. Описание почтовых заголовков

Почтовый заголовок	Значение заголовка	Индикатор	Описание индикатора
X-Distribution	bulk	Наличие заголовка X-Distribution со значением bulk	Письмо адресовано большому количеству получателей. Присутствие данного заголовка чаще всего свидетельствует о спам-рассылках.
Bcc	Есть данные	Наличие заголовка Bcc	Заголовок скрытой копии. Это признак плохо написанного заголовка. Заголовок Bcc обрабатывается и удаляется на SMTP-сервере отправителя.
X-UIDL	Есть данные	Наличие заголовка X-UIDL	Входящие сообщения не должны иметь заголовка X-UIDL, поскольку они предназначены только для почтового сервера. Он обычно удаляется при получении сообщения. Это признак плохо написанного заголовка.

Почтовый заголовок	Значение заголовка	Индикатор	Описание индикатора
Received	Разница дат	Большая задержка в приеме электронной почты	Временной интервал больше 5 минут при получении письма может указывать на перегруженный почтовый сервер рассылки спама.
	Код страны из black list	Подозрительный путь письма	Письмо прошло через сервер страны, в которой замечен высокий уровень фишинговых атак.
To	Нет данных	Отсутствие адреса получателя	Отсутствие адреса получателя в заголовке «To» характерно для спам-рассылок.
	Нет данных	Отсутствие получателей	В заголовке «To» отсутствуют какие-либо почтовые адреса, что характерно для спам-рассылок.
	Более 10 адресов	Большое число получателей	Письмо предназначено для более 10 получателей, что характерно для спам-рассылок.
Message-ID	-	Отсутствует заголовок Message-ID	Отсутствие заголовка Message-ID характерно для спам-рассылок.
Return-Path	Не равен полю «From»	Некорректный адрес возврата письма	Если адрес возврата письма не совпадает с адресом отправителя в поле «From», это значит, что отправитель скрывает адрес рассылки.

Почтовый заголовок	Значение заголовка	Индикатор	Описание индикатора
Reply-To	Не равен полю «From»	Некорректный адрес для ответа	Если адрес для ответа не совпадает с адресом отправителя в поле «From», это значит, что злоумышленники скрывают адрес рассылки.
From	Равен полю «To»	Совпадение адресов отправителя и получателя	Если адрес отправителя совпадает с адресом получателя в поле «To», это значит, что злоумышленники скрывают адрес рассылки.

Во вкладке «Файлы» отчета отображаются все вложения в письме, которые проверяются на наличие вредоносного контента по антивирусной базе данных Системы (Рисунок 16).

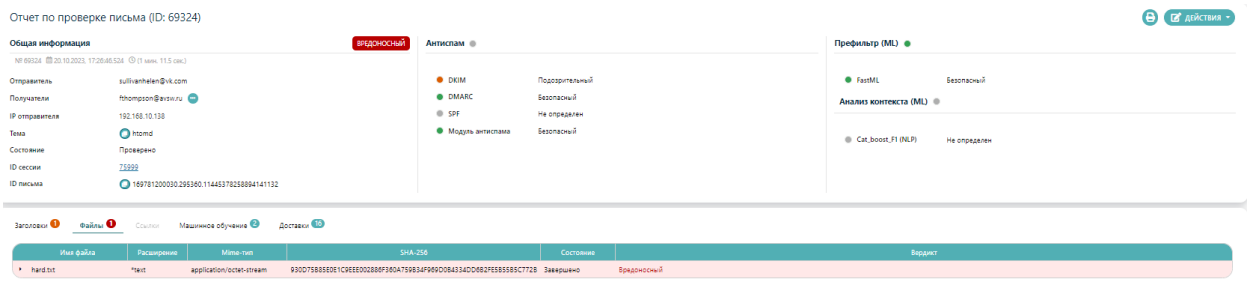

Рисунок 16. Отчет по проверке на спам, вкладка «Файлы»

Каждый из обнаруженных файлов исследуется Системой и, в зависимости от его вредоносности, получает вердикт: безопасный, подозрительный или вредоносный.

Во вкладке «Ссылки» отображаются все исследования, взятые от ссылок, обнаруженные в письме и проанализированные Системой (Рисунок 17).

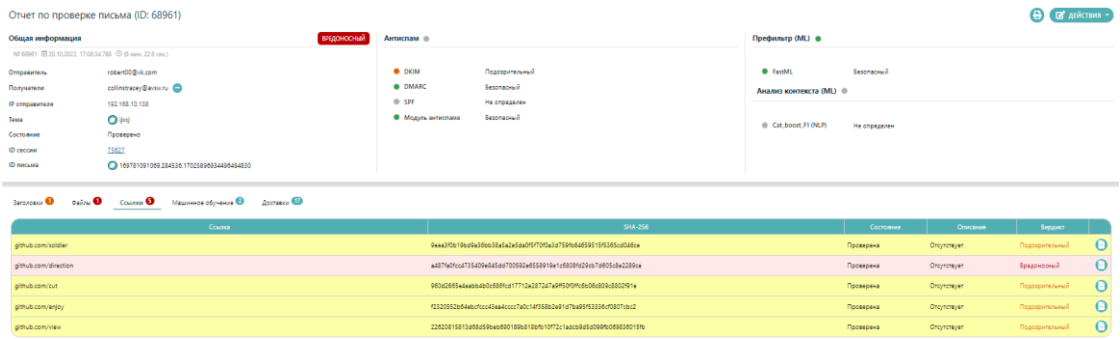

Рисунок 17. Отчет по проверке письма, вкладка «Ссылки»

Есть возможность предпросмотра скриншотов исследования ссылки из Афины в таблице исследования ссылок (Рисунок 18)

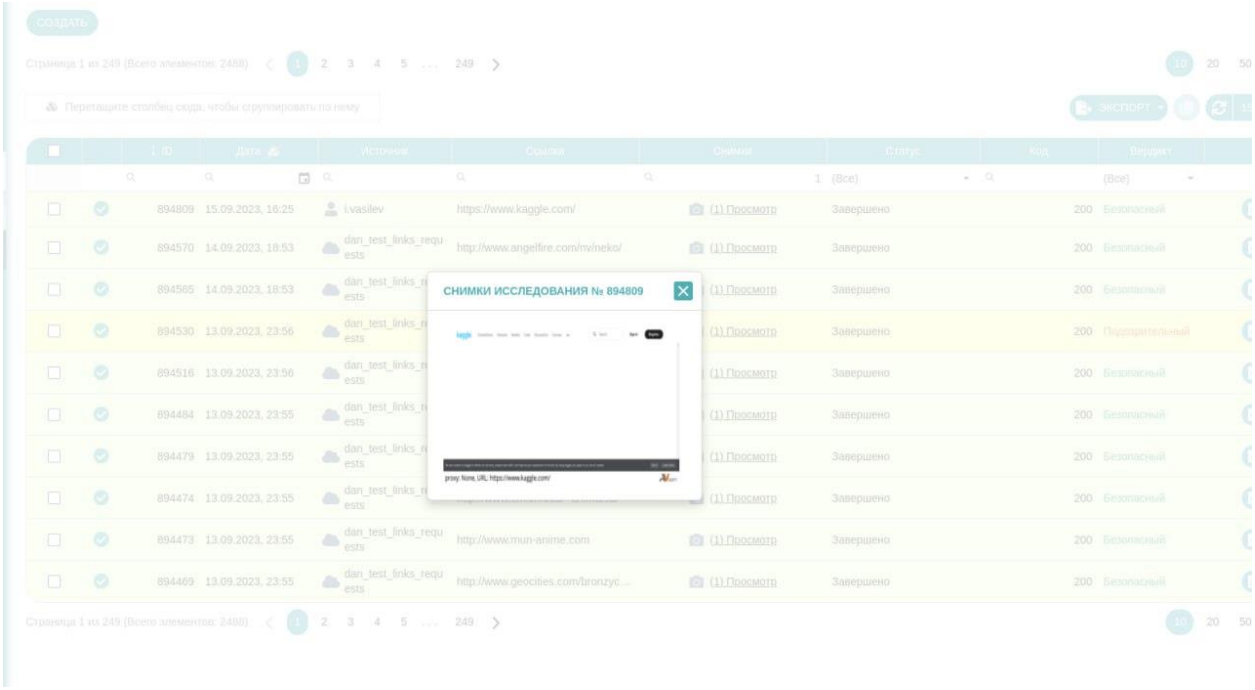

Рисунок 18. Предпросмотр скриншота исследования

Каждая из обнаруженных ссылок исследуется Системой и, в зависимости от ее вредоносности, получает вердикт: безопасный, подозрительный или вредоносный. Результат исследования ссылки, обосновывающий ее вердикт, можно посмотреть, пройдя по интерактивной иконке отчета напротив ссылки (Рисунок 19).

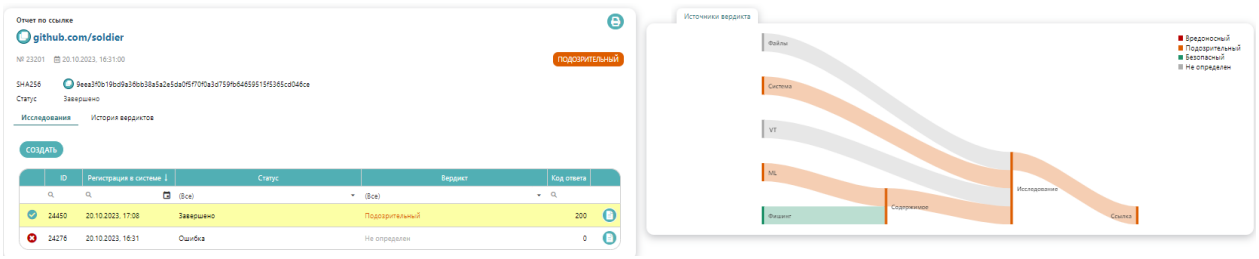

Рисунок 19. Отчет по исследованию ссылки

Итоговый вердикт письма формируется на основании наивысшего по вредоносности вердикта его блоков анализа. Есть вердикт от Virus Total в дерево вердиктов в отчет по исследованию ссылки.

Итоговый вердикт отчета по проверке письма может быть принудительно изменен в ручном режиме. Для этого на странице отчета надо нажать на кнопку «Действия» (Рисунок 20).

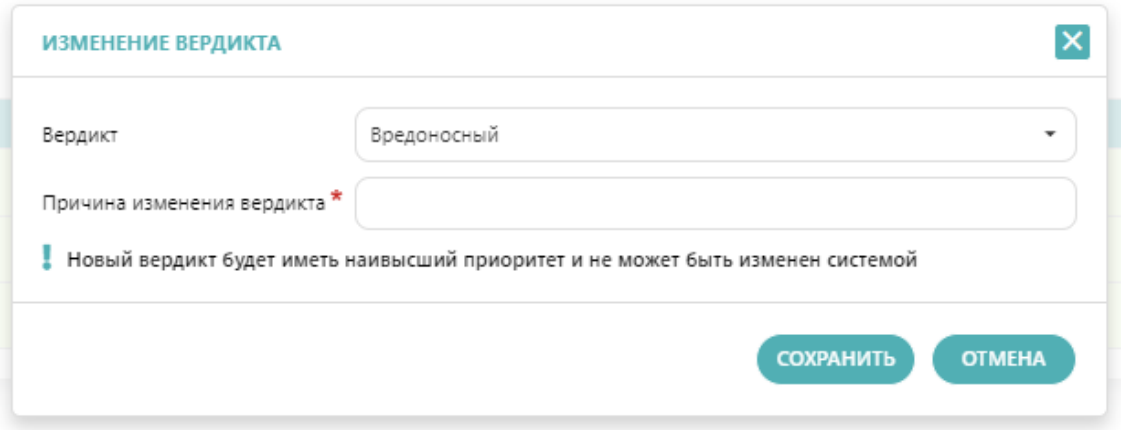

Рисунок 20. Форма изменения вердикта

В открывшейся форме следует указать новый вердикт и причину его изменения. После чего нажать на кнопку «Сохранить». Вердикт, установленный вручную, имеет в системе наивысший приоритет и может быть изменен только в ручном режиме.

6.4 Машинное обучение

Во вкладке «Машинное обучение» отображаются результаты проверки письма на спам моделями машинного обучения. В анализе используются NLP-модели и модели-трансформеры, которые извлекают текст из письма и переводят его в векторное представление слов (англ., embedding).

Для анализа используются две модели ML. Первая - табличная модель CatBoost, которая анализирует извлеченный из письма эмбеддинг и классифицирует его по двум категориям: Спам / Не спам. Вторая модель, с использованием методов полу-контролируемого обучения, определяет категорию контента письма (рассылка, знакомства, деловая переписки и т.д.). Всего модель использует более 55 различных категорий. Выявленные категории отображаются в параметре «Категории» отчета. На основании выявленных категорий письму присваиваются соответствующие теги в системе, которые перечисляются в параметре «Теги» отчета (Рисунок 21).

Рисунок 21. Отчет оп проверке письма, вкладка «Машинное обучение»

Пороги отнесения письма к спаму являются настраиваемыми. Величина порогов ML, предустановленных в системе, отображена в таблице 10.

Таблица 10. Пороги ML

Порог ML	Формируемый вердикт
0 – 85.0 %	безопасный
85.1 – 99.0 %	подозрительный
99.1 – 100 %	вредоносный

6.5 Доставка

Во вкладке «Доставки» отображается информация об адресах, на которые были доставлены письма (Рисунок 22)

Рисунок 22. Вкладка «Доставки»

6.6 SMTP-сессии

Во вкладке «SMTP-сессии» отображается история соединений по SMTP сессии и их статус (Рисунок 23).

Рисунок 23. Вкладка «SMTP-сессии»

7 Политики

7.1 Первичная проверка

Таблица «DNSBL» содержит список доверенных внешних ресурсов, которые осуществляют проверку на спам. Для того чтобы добавить запись в таблицу нужно нажать на кнопку «Добавить». Появится форма для заполнения параметров (Рисунок 24).

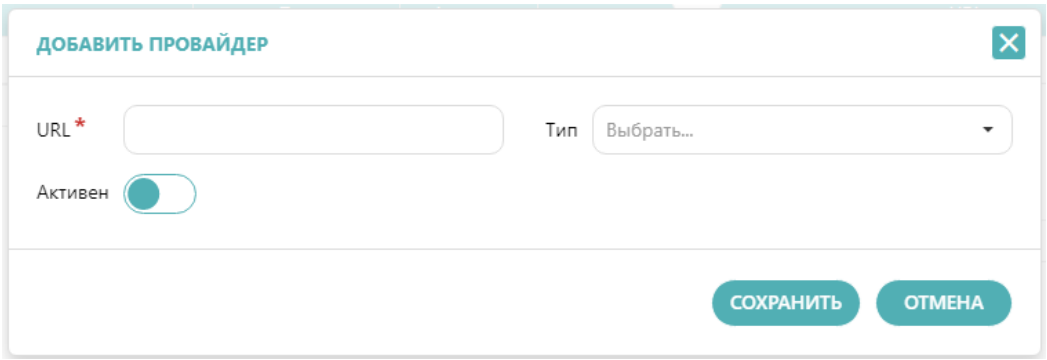

Рисунок 24. Форма добавления провайдера

В открывшейся форме необходимо указать параметры, описанные в таблице 11.

Таблица 11. Параметры добавления нового провайдера

№	Параметры	Описание
1.	URL	Адрес внешнего ресурса, который осуществляет проверку на спам.
2.	Тип	Выбор типа проверки репутации. Например, можно спросить выбранного провайдера (по его URL), что он думает об этом IP адресе, а другого, что он думает об этом email

№	Параметры	Описание
		отправителя, обычно один провайдер отвечает только на один тип проверки. Всего на выбор предоставляется два типа: – Домен, то есть, проверка репутации по email отправителя; – IP адрес.
3.	Активен	Флаг, при активации которого доверенный ресурс будет осуществлять проверку на спам.

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новый провайдер отобразился в таблице.

Таблица «Исключения проверки DNSBL» позволяет настроить политики блокировки для указанного домена или IP-адреса. Связана с таблицей «DNSBL». Указанные в таблице «Исключения проверки DNSBL» адреса не проверяются на внешних ресурсах таблицы «DNSBL», а сразу блокируется в соответствии с политикой, которая указана в самой таблице «Исключения проверки DNSBL».

Для добавления новой политики нужно нажать на активную кнопку «Добавить» и появится окно для указания параметров политики (Рисунок 25).

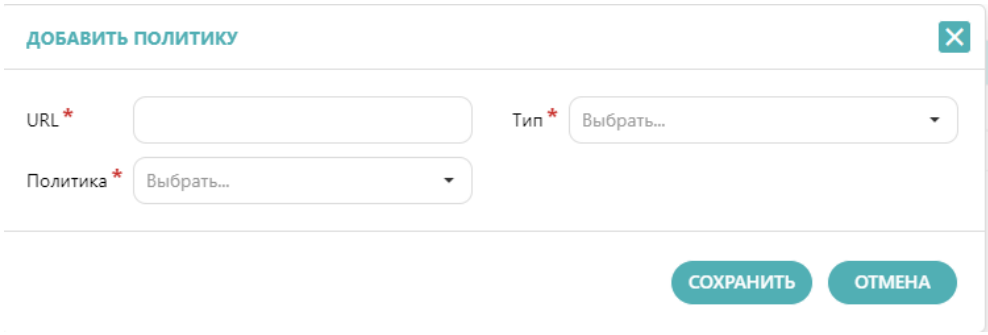

Рисунок 25. Форма добавления политики

В открывшейся форме необходимо указать параметры, описанные в таблице 12.

Таблица 12. Параметры добавления новой политики

№	Параметры	Описание
1.	URL	Адрес внешнего ресурса.
2.	Тип	Выбор типа проверки репутации. Всего на выбор предоставляется два типа: – Домен, то есть, проверка репутации по email отправителя; – IP адрес.
3.	Политика	Выбор действия для заданной политики («Разрешить» или «Заблокировать»).

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новая политика отобразилась в таблице.

Во вкладке «Сессии» отображаются сессионные профили. Для добавление нового профиля нужно нажать на кнопку «Добавить» и настроить ограничения под профиль, указав перед этим IP. Есть возможность настраивать проверки, используя флаги. (Рисунок 26 и Рисунок 27)

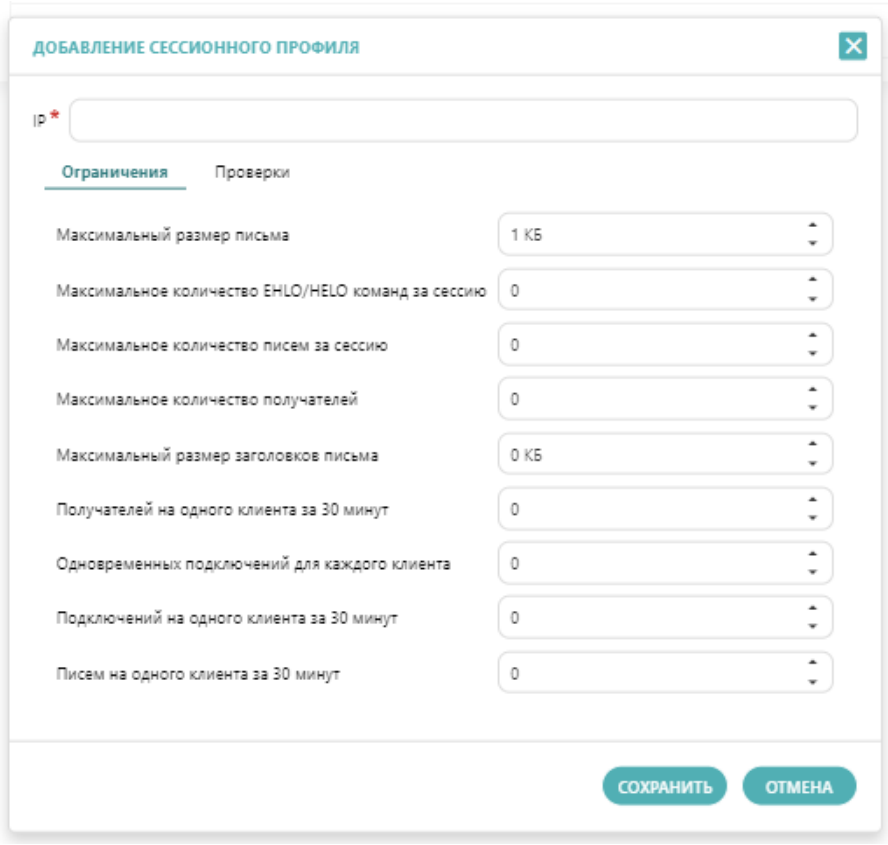

Рисунок 26. Добавление сессионного профиля

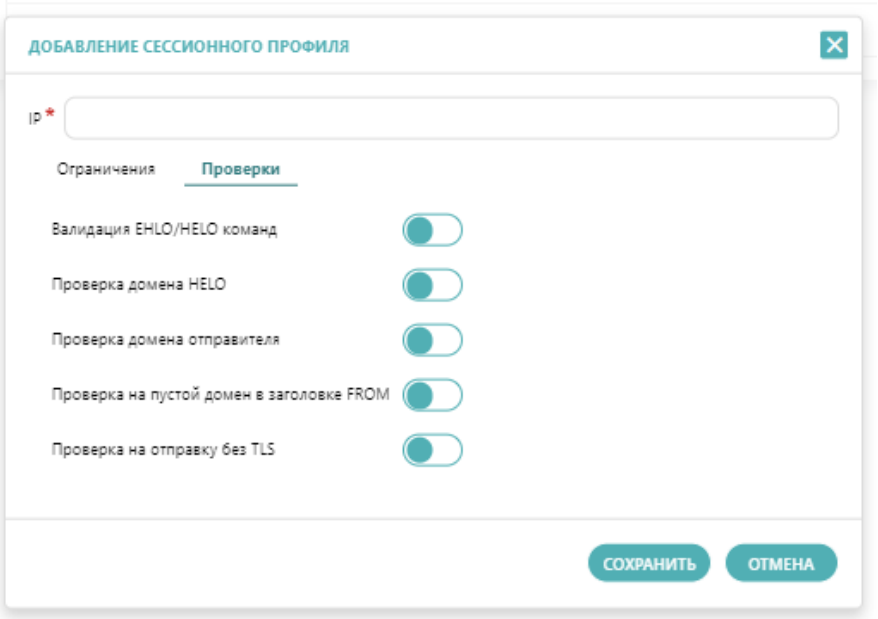

Рисунок 27. Добавление проверок в сессионном профиле

Таблица «Пользователи LDAP» позволяет настроить поиск указанного почтового ящика на сервере. Если email адрес получателя не получается найти хотя бы на одном сервере, то письмо будет отвергнуто.

Для добавления новой записи LDAP нужно нажать на активную кнопку «Добавить» и появится окно для указания параметров (Рисунок 28).

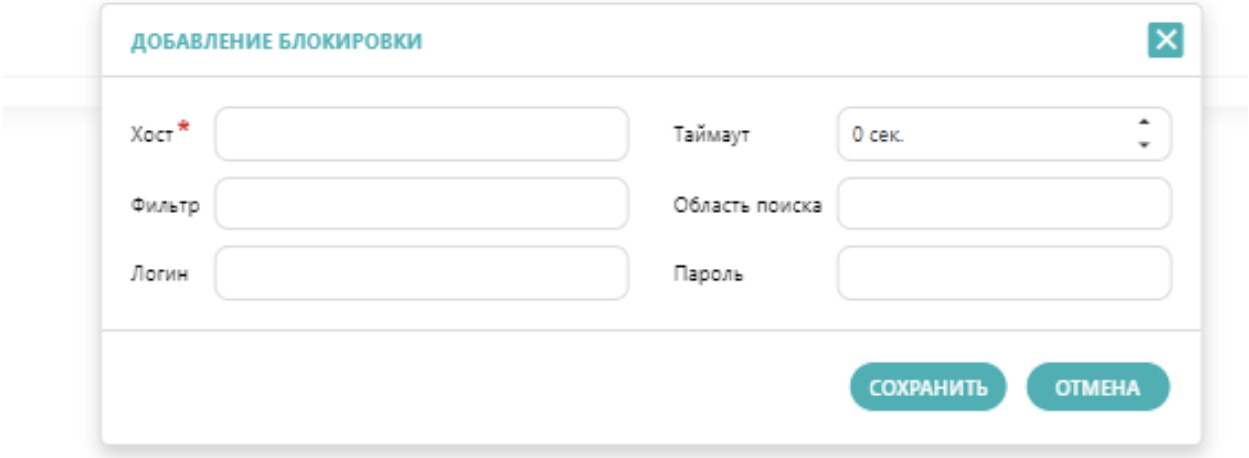

Рисунок 28. Форма добавления LDAP

В открывшейся форме необходимо указать параметры, описанные в таблице 13.

Таблица 13. Параметры добавления новой записи LDAP

№	Параметры	Описание
1.	Хост	IP-адрес проверяемого email получателя.
2.	Фильтр	Основное выражение, по которому принимается решение, то есть если производить запрос на AD, и искать получателя по фильтру, если его находим, то письмо принимается, если нет, то отвергается, (доступна переменная %mail%, чтобы использовать email получателя).
3.	Логин	Логин хоста.
4.	Таймаут	При достижении таймаута, почтовый адрес считается не найденным и письмо, которое было отослано на несуществующий адрес, блокируется (в секундах).
5.	Область поиска	Параметр для того, чтобы сузить область поиска по фильтру.
6.	Пароль	Пароль хоста.

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новая запись отобразилась в таблице.

Проверки во вложенной вкладки «Блокировки» происходят последовательно, сначала DNSBL или «Политики», потом LDAP. Письмо может быть заблокировано на любом этапе.

Во вкладке «Серый список» находятся исключения серого списка. Имеется возможность редактирования уже готовые записи, удалять, а также добавлять новые и настраивать список (Рисунок 29)

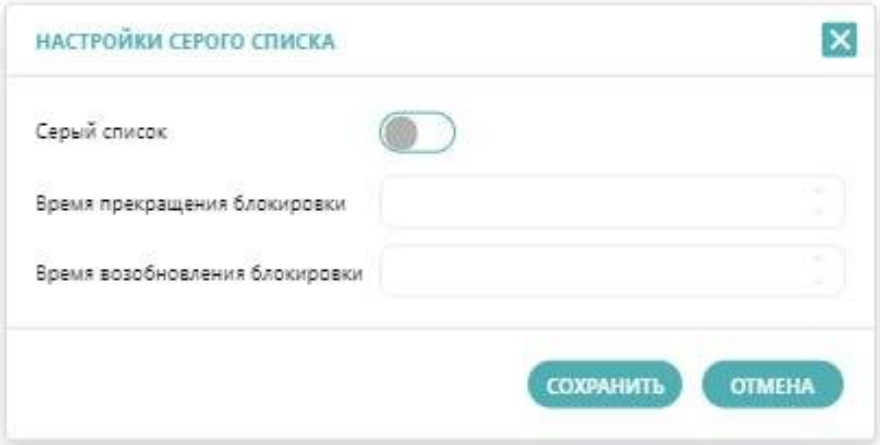

Рисунок 29. Настройка серого списка

7.2 Профили

Во вкладке «Профили» настраивается использование политик в отношении различных отправителей и получателей почты (Рисунок 30).

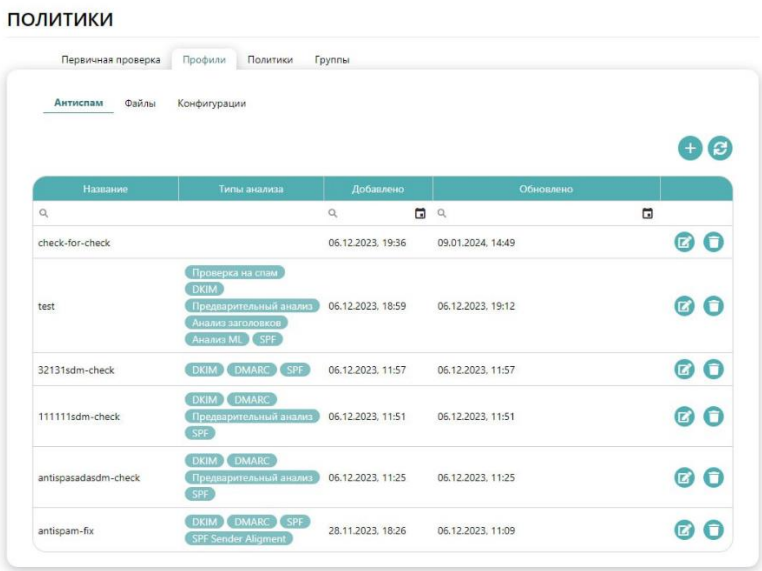

Рисунок 30. Список профилей почтового трафика

Во вкладке «Профили» - «Антиспам» настраиваются виды проверок, на основе которых добавляются профили, а также отображается информация о

включенных типах анализа. Для добавления новой политики проверки антиспамов нужно нажать на активную кнопку «Добавить». После этого откроется окно, где необходимо ввести данные (Рисунок 31)

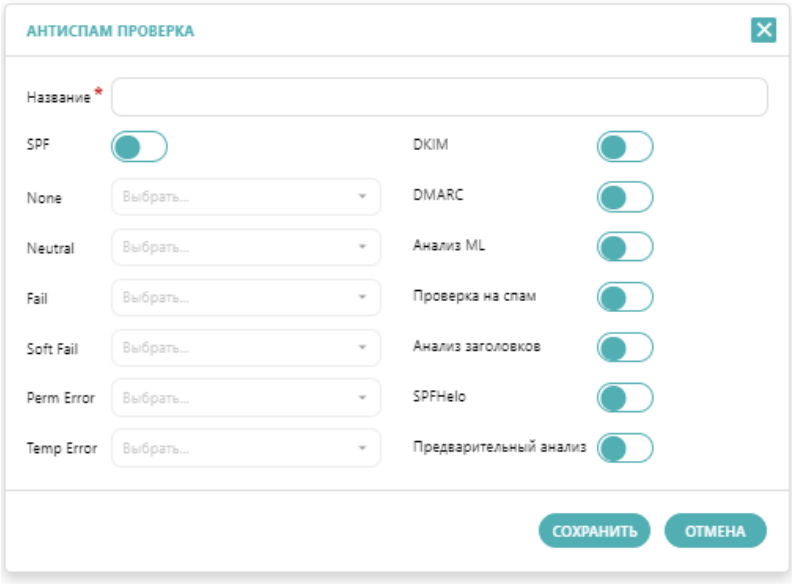

Рисунок 31. Антиспам проверка

В открывшейся форме необходимо указать параметры, описанные в таблице 14.

Таблица 14. Параметры настройки антиспам проверки

№	Параметры	Описание
1.	Название	Указывается название политики
2.	SPF	Флаг, активирует метод SPF, который определяет статус прав отправителя сообщений (есть ли право отправителя отправлять сообщение от имени домена или нет) по данным из заголовков сообщений.
3.	None	Выбор параметра указывает либо игнорировать, либо запретить игнорировать (т.е. учитывать) доставку сообщений, которые не прошли проверку на SPF
4.	Neutral	Выбор параметра указывает либо игнорировать, либо запретить игнорировать (т.е. учитывать) работу нейтрального режима. В нейтральном режиме можно отправлять и

№	Параметры	Описание
		получать сообщение не авторизированным IP - адресам
5.	Fail	Выбор параметра указывает либо игнорировать, либо запретить игнорировать (т.е. учитывать) выполнение команды отбросить сообщение, исходящие от любого источника отправки, который не указан SPF-записи.
6.	Soft Fail	Выбор параметра указывает либо игнорировать, либо запретить игнорировать (т.е. учитывать) назначение вердикта спам, если IP-адрес не указан в SPF-записи
7.	Perm Error	Выбор параметра указывает либо игнорировать, либо запретить игнорировать (т.е. учитывать) постоянную ошибку DNS сервера во время проверки. Причина ошибки DNS сервера: - превышение запросов по лимиту (свыше 10); - неправильный синтаксис записи SPF; - более одной записи SPF для одного и того же домена; - превышение предела длины записи SPF в 255 символов
8.	Temp Error	Выбор параметра указывает либо игнорировать, либо запретить игнорировать (т.е. учитывать) временную ошибку DNS сервера во время проверки. При повторном запросе DNS сервер ошибки не выдаст.
9.	DKIM	Флаг, при активации которого выполняется аутентификация отправителя письма т.е. DNS сервер проверяет правильность подписи отправителя при помощи публичного ключа.

№	Параметры	Описание
10.	DMARC	Флаг, при активации которого выполняется проверка подлинности отправителя письма с использованием механизмов DKIM и SPF. Назначение окончательного вердикта «вредоносный», если DKIM или SPF вредоносные.
11.	Анализ ML	Флаг, при активации которого выполняется функция фильтрации на спам сообщения и не спам сообщения из общего числа для возможности минимизации обработки сообщений системой
12.	Проверка на спам	Флаг, при активации которого выполняется проверка встроенным антиспам движком
13.	Анализ картинок	Флаг, при активации которого выполняется проверка вложенных картинок
14.	Анализ заголовков	Флаг, при активации которого выполняется проверка заголовков на подозрительные или вредоносные индикаторы
15.	SPFHelo	Флаг, активирует метод SPFHelo, который определяет статус прав отправителя сообщений (есть ли право отправителя отправлять сообщение от имени домена или нет) по данным из smtp сессии.
16.	Предварительный анализ	Флаг, при активации которого выполняется функция ML которая оперативно отсеивает наиболее вероятный спам сообщений

Во вкладке «Профили» - «Файлы» осуществляется настройка политик интеграции с песочницей ATHENA для проверки вложенных файлов в письме (Рисунок 32)

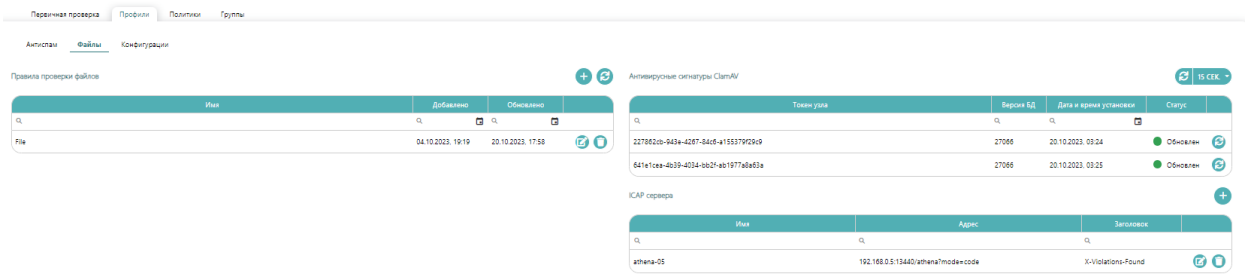

Рисунок 32. Вкладка «Файлы»

Имеются флаги для блокировки файлов/архивов в модальном окне создания/редактирования политики проверки файлов.

Для добавления нового правила проверки файлов нужно нажать на активную кнопку «Добавить». После этого откроется окно, где необходимо указать правила проверки файлов (Рисунок 33).

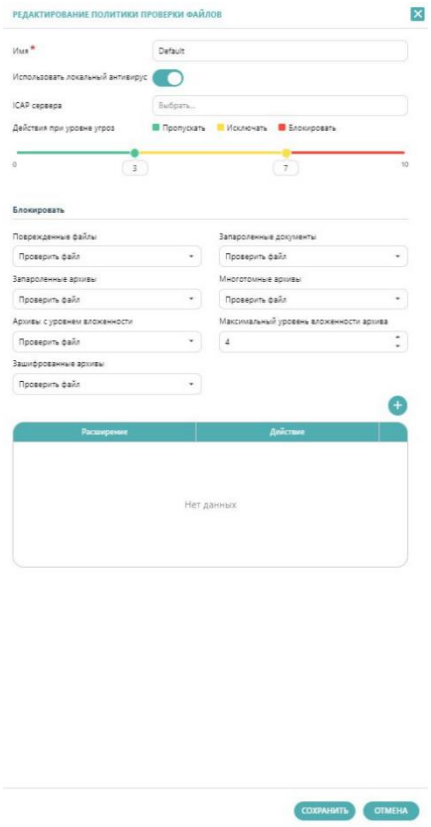

Рисунок 33. Окно добавление новой политики проверки файлов

В открывшейся форме необходимо указать имя, выбрать условия блокировки, уровень угрозы, использование локального антивируса, а также ICAP сервера. Имеется возможность добавления действий по расширениям.

В таблице «Антивирусные сигнатуры ClamAV» находится список сигнатур, который может содержать несколько строк, по строке для каждой ноды, обновление баз данных происходит ежедневно.

В таблице ICAP сервера есть возможность редактирования уже имеющихся адресов и добавление новых.

Во вкладке «Профили» - «Конфигурации» располагается антиспам профилей. (Рисунок 34)

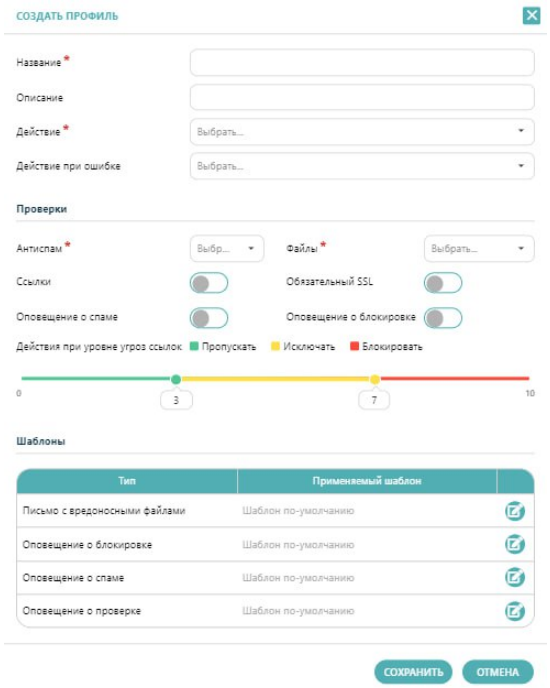

Рисунок 34. Вкладка «Конфигурации»

В открывшейся форме необходимо указать параметры, описанные в таблице 15

Таблица 15. Параметры конфигурации

№	Параметры	Описание
1.	Название	Указывается название профиля
2.	Описание	Указывается описание профиля
3.	Действие	Выбирается действие, которое будет присвоено профилю из следующих: – Пропускать все письма – Проверять письма – Блокировать письма

№	Параметры	Описание
4.	Действие при ошибке	Выбирается действие при ошибке из следующих: – Пропускать – Блокировать

Также есть возможность настройки проверки, уровня угроз ссылок и шаблонов и возможность поиска конфигурации по названию или описанию, которое было задано при создании (Рисунок 35).

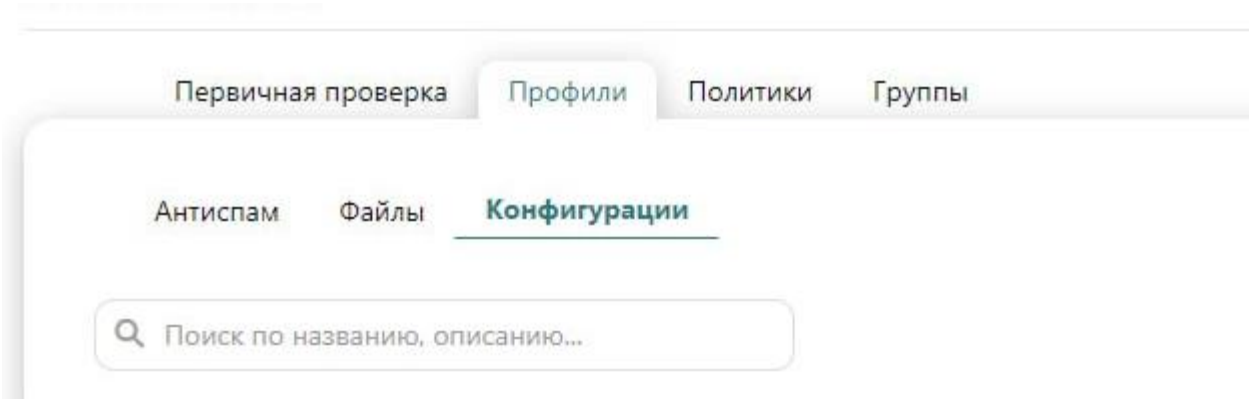

Рисунок 35. Поле ввода для поиска конфигурации по названию

7.3 Политики

Во вкладке «Политики» настраиваются правила проверок почтового трафика (Рисунок 36).

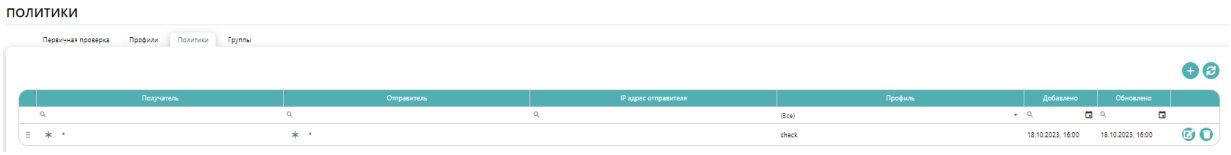

Рисунок 36. Вложенная вкладка "Политики"

Для добавления новой политики необходимо нажать кнопку «Добавить», которая отобразит форму для заполнения «Политики» (Рисунок 37).

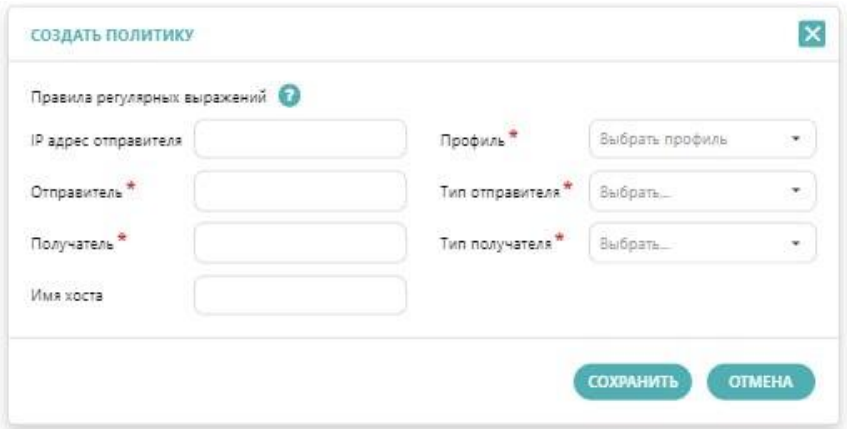

Рисунок 37. Форма «Политика»

В открывшейся форме необходимо указать параметры, описанные в таблице 16:

Таблица 16. Параметры создания политики

№	Параметры	Описание
1.	Тип отправителя	Выбрать один из параметров, либо регулярное выражение, либо метасимволы (Wildcard), либо группу пользователей в зависимости от того, как будет задаваться почтовый адрес отправителя. Например: 1) почтовый адрес отправителя планируется задать регулярным выражением в таком случае требуется выбрать регулярное выражение. 2) почтовый адрес отправителя планируется задать метасимволами в таком случае требуется выбрать Wildcard. 3) почтовый адрес отправителя планируется задать группе в таком случае требуется выбрать группа пользователей.
2.	Имя хоста	Заносится имя хоста
3.	Тип получателя	Выбрать один из параметров, либо регулярное выражение, либо метасимволы (Wildcard), либо группу получателей в зависимости от того, как будет задаваться почтовый адрес получателя. Например: 1) почтовый адрес получателя планируется задать регулярным выражением в таком случае требуется выбрать

№	Параметры	Описание
		регулярное выражение. 2) почтовый адрес получателя планируется задать метасимволами в таком случае требуется выбрать Wildcard. 3) почтовый адрес получателя планируется задать группе в таком случае требуется выбрать группа пользователей.
4.	Отправитель	Указывается почтовый адрес отправителя. Можно задать при помощи регулярного выражения, метасимволов или выбрать сформированную группу пользователей в зависимости от выбранного параметра «тип отправителя»
5.	Получатель	Указывается почтовый адрес получателя. Можно задать при помощи регулярного выражения, метасимволов или выбрать сформированную группу получателей в зависимости от выбранного параметра «тип получателя»
6.	IP адрес отправителя	IP адрес отправителя.
7.	Профиль	Политика, которая будет использоваться для заданных отправителей и получателей.

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новая политика отобразилась в общей таблице политик.

Так же в окне добавления новой политики находится активная иконка в виде вопроса, при нажатии на которую будет отображено подробное описание общих правил составления регулярных выражений (Рисунок 38).

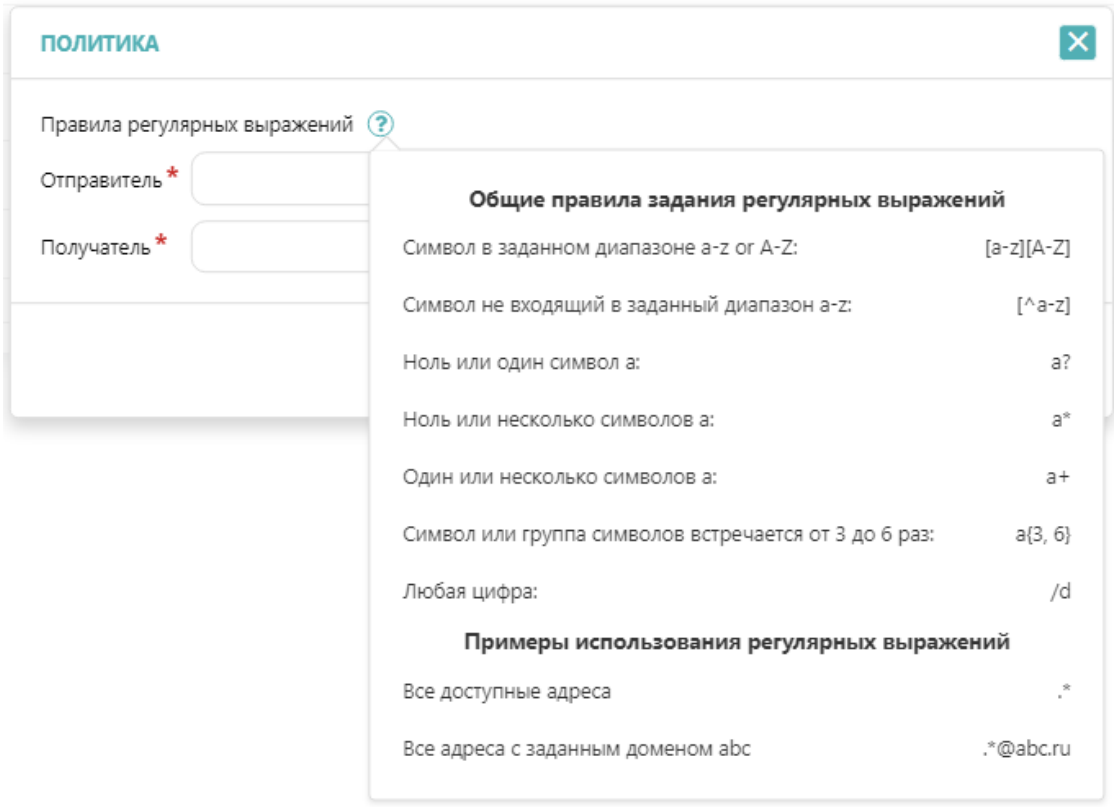

Рисунок 38. Подробное описание написания правил регулярных выражений

7.4 Группы

Во вложенной вкладке «Группы» осуществляется создание и настройка групп пользователей. Группы можно создать по признаку почтовых адресов, IP-адресов или ключевых слов (Рисунок 39).

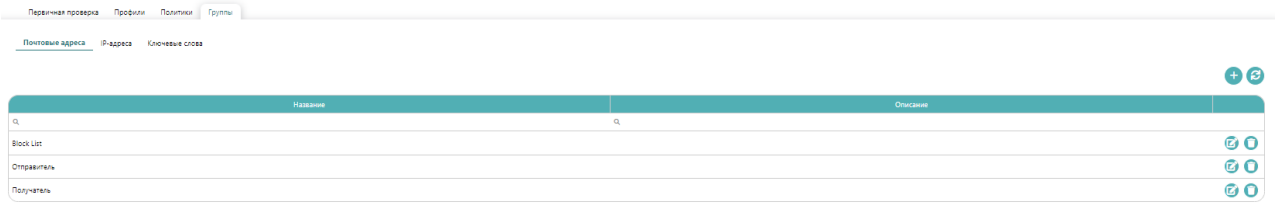

Рисунок 39. Группы почтовых пользователей

Для создания новой группы необходимо нажать на кнопку «Добавить», которая отобразит форму для заполнения (Рисунок 40).

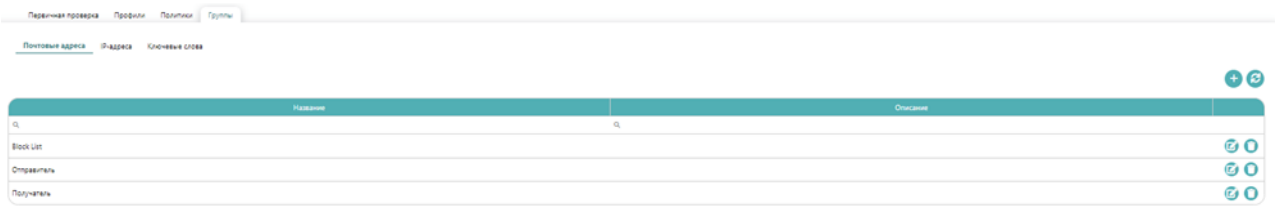

Рисунок 40. Форма «Настройки обработки писем группы»

В окне «Настройка обработки писем группы» необходимо указать параметры, описанные в таблице 17.

Таблица 17. Параметры создания новой группы получателей

№	Параметры	Описание
1.	Название	Название группы получателей электронных писем с вложениями.
2.	Описание группы	Краткое идентификационное описание группы.

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

При редактировании группы необходимо указать новое название, описание и шаблон, по которому данная группа будет формироваться (Рисунок 41)

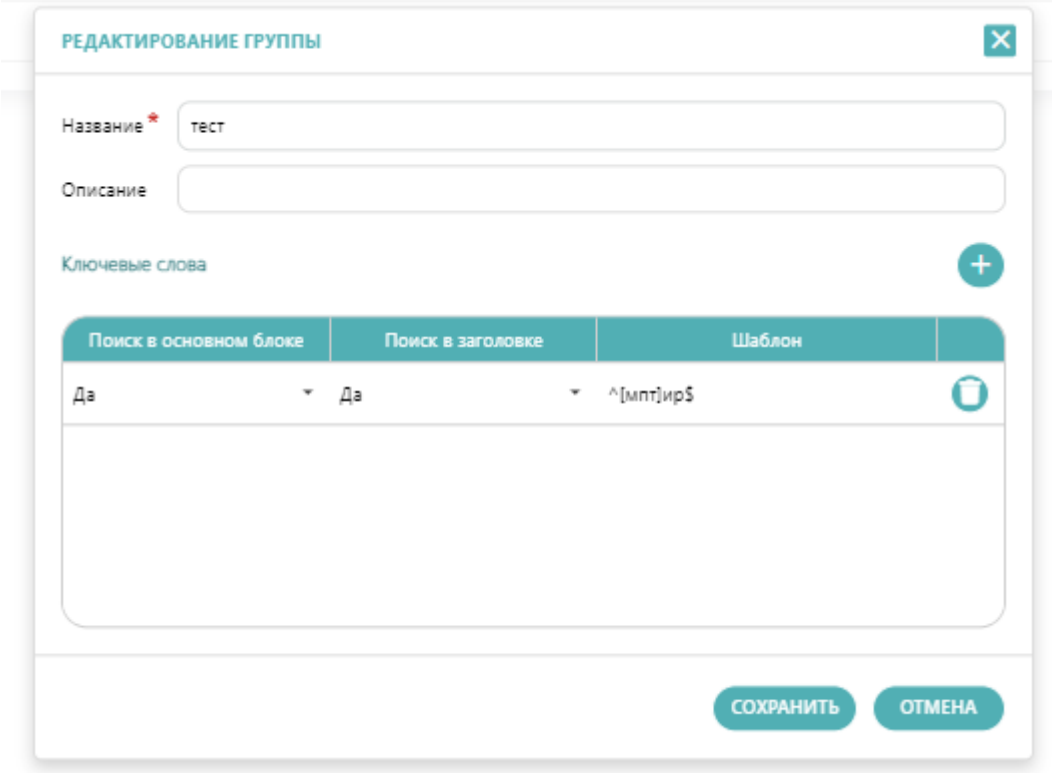

Рисунок 41. Редактирование группы

8 Раздел «Ссылки»

8.1 Ручной режим исследования ссылки

Инициация исследования ссылок в системе может осуществляться в ручном и автоматическом режиме.

В автоматическом режиме исследования ссылок создаются без участия пользователя по заранее заданному сценарию, который указывается в настройках администратором при интеграции источника проверки в систему.

В ручном режиме пользователь самостоятельно осуществляет загрузку и запуск исследований по интересующим его параметрам. Для начала исследования необходимо загрузить объект проверки в систему одним из следующих способов:

– Кнопкой «Проверить» в верхней панели системы;

– Кнопкой «Создать» в разделе «Исследования».

При выборе способа загрузки при помощи кнопки «Загрузка ссылки» отобразится форма «Загрузка на проверку», в которую нужно вставить проверяемую ссылку. По окончании ввода необходимо нажать кнопку «Запустить» (Рисунок 42).

Рисунок 42. Форма загрузки ссылки

Флаг «Использовать TOR» применяется, если нужно инициировать исследование с использованием сети TOR. Переход по ссылке будет осуществляться не с использованием IP заказчика, а с применением узла TOR.

При выборе способа загрузки ссылки при помощи кнопки «Создать» в разделе «Ссылки» отобразится форма «Создание исследования ссылки», в которую следует вставить проверяемую ссылку и указать в поле «Типы исследования ссылки» используемые в проверке модули, а в поле «Параметры исследования ссылки» выбрать нужные параметры (Исследование переходов, семантический анализ URL или анализ скриншотов) из выпадающего меню. По окончании ввода данных необходимо нажать кнопку «Запустить» (Рисунок 43).

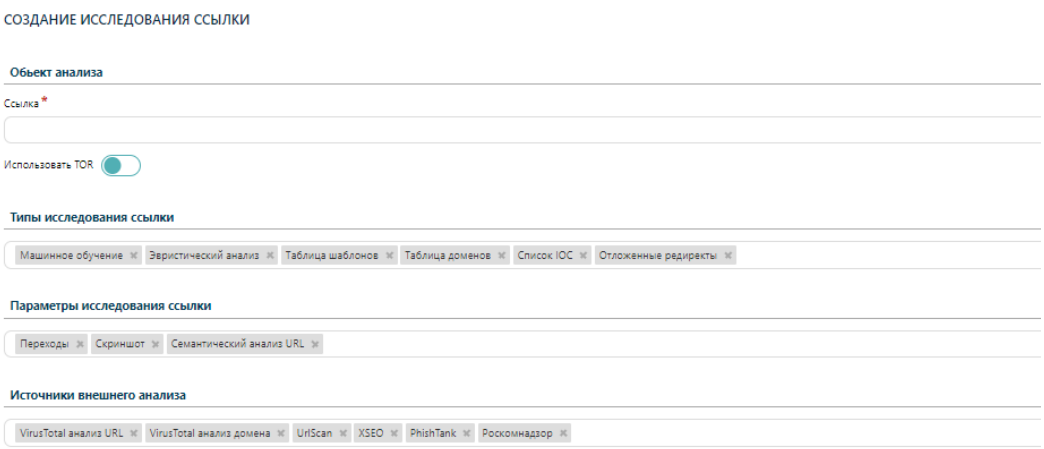

Рисунок 43. Форма создания исследования ссылки

8.2 Отчет по ссылке

В общей таблице ссылок отображаются все ссылки, прошедшие проверку в Системе. В таблице присутствует цветовая индикация вердикта ссылок: безопасный вердикт – зеленый цвет, подозрительный вердикт – желтый цвет, вредоносный вердикт - красный цвет (Рисунок 44).

Рисунок 44. Таблица ссылок

По каждой ссылке можно просмотреть отчет, обосновывающий присвоенный ей вердикт, нажав на иконку «Отчет» (Рисунок 45).

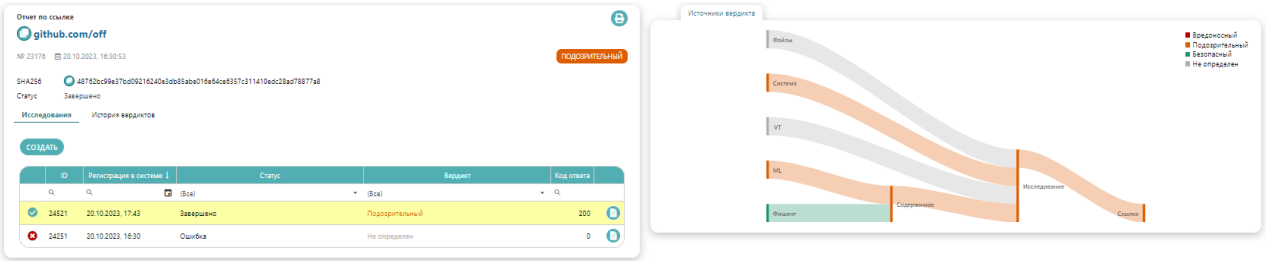

Рисунок 45. Отчет по ссылке

Для более детального ознакомления с результатами исследования ссылки необходимо перейти в отчет по исследованию, нажав на иконку «Отчет» вкладки «Ссылка» в отчете по ссылке (Рисунок 48).

Также система предоставляет возможность изменения вердикта ссылки в ручном режиме при ложном срабатывании. Для этого необходимо нажать на иконку «Изменить вердикт» напротив нужной ссылки и заполнить все требуемые поля в открывшейся форме (Рисунок 46). Вердикт, установленный вручную, имеет в системе наивысший приоритет и может быть изменен только в ручном режиме.

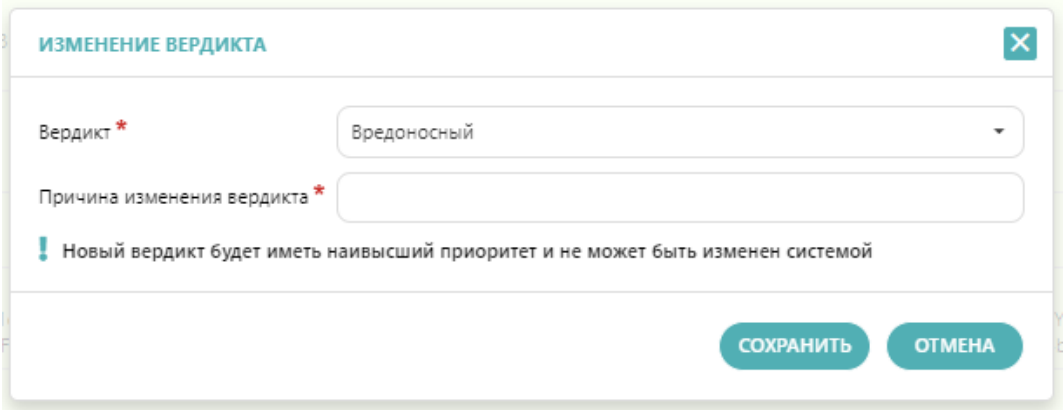

Рисунок 46. Форма изменения вердикта

В таблице ссылок можно отслеживать статусы исследования ссылок (Рисунок 47). Для проведения повторного анализа ссылки надо нажать на иконку «Копировать» напротив нужной ссылки и запустить исследование.

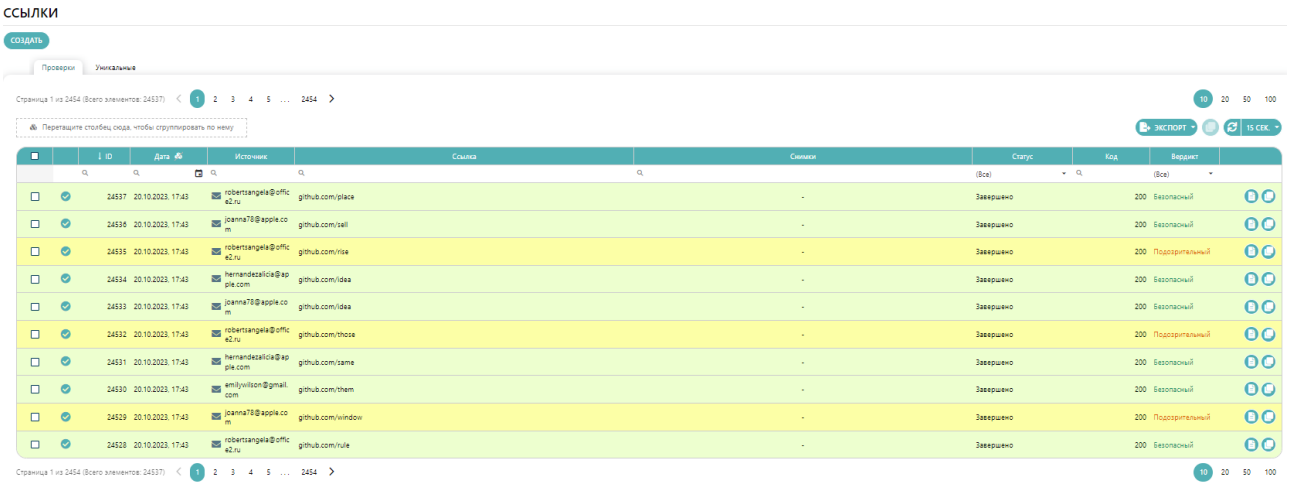

Рисунок 47. Раздел «Проверки»

По каждому проведенному исследованию можно просмотреть отчет, нажав на иконку «Отчет» напротив нужного исследования (Рисунок 48).

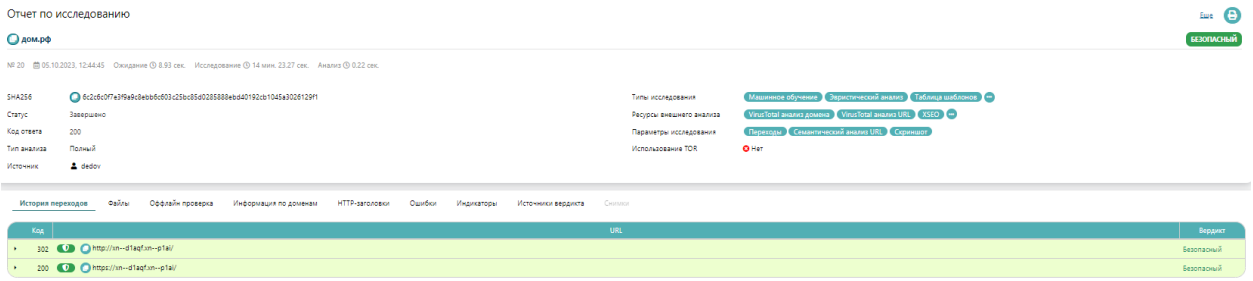

Рисунок 48. Отчет по исследованию

Отчет по исследованию ссылки включает в себя параметры, описанные в таблице 18.

Таблица 18. Параметры отчета по исследованию

№	Параметр	Описание
1.	Общая информация	Значимые идентификационные параметры ссылки: – имя; – номер исследования; – дата и время запуска исследования; – длительность
2.	Вердикт	Итоговый вердикт по ссылке в системе на основании всех источников анализа
3.	SHA256	Контрольная сумма ссылки, которая может использоваться в качестве ее уникального идентификатора для поиска информации о ней во внешних аналитических ресурсах и для безопасной передачи информации о ссылке
4.	Типы исследования	Указание типа исследования ссылки в виде тега
5.	Параметры исследования	Указание параметров исследования в отчете в виде тега
6.	Источник	Источник поступления ссылки на проверку в систему
7.	Статус	Статус исследования ссылки в системе

№	Параметр	Описание
8.	Использование TOR	Индикатор применения анонимизации трафика при переходе по ссылке
9.	Версия анализа	Версия модуля анализа ссылок, используемого для анализа в системе
10.	Код ответа	Ответ сервера при запросах по протоколу HTTPS
11.	История переходов	Все возможные переходы по веб-ссылке и результаты их анализа внешними аналитическими ресурсами и моделями машинного обучения
12.	Файлы	Файлы, которые находились внутри ссылки и были проверены в системе.
13.	Оффлайн проверка	Результат проверки ссылки локальными базами данных и моделями ML, которым не требуется доступ в Интернет
14.	Информация по доменам	Раскрывается детальная информация домена с указанием: IP-адреса, владельца, расположение и др.
15.	HTTP-заголовки	Информация о заголовках веб-ресурса
16.	Ошибки	Перечень ошибок модулей анализа во время проверки ссылки
17.	Индикаторы	Перечень и описание системных индикаторов, отработавших в результате проверки ссылки
18.	Источники вердикта	Графическое представление результата формирования вердикта ссылке блоками анализа
19.	Снимки	Снимки экрана при отображении веб-страницы

8.3 Анализ машинного обучения

При анализе ссылки на фишинг, наряду с использованием внешних аналитических ресурсов, используется машинное обучение. Машинное обучение включает в себя несколько моделей с разными типами алгоритмов.

Эта информация доступна при нажатии на значок раскрывающегося списка (Рисунок 49).

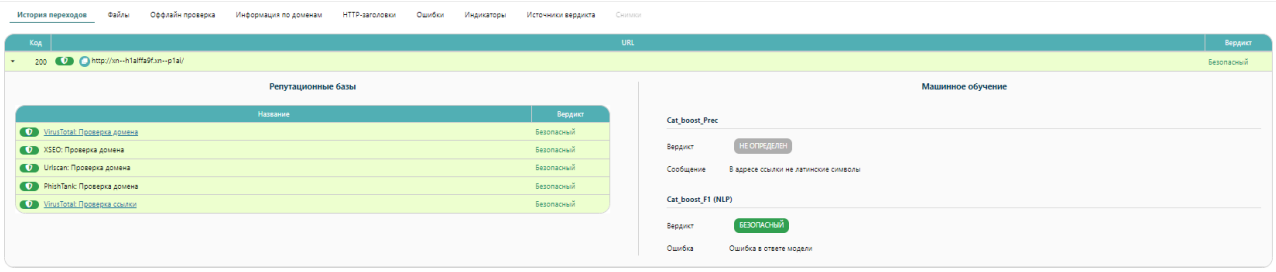

Рисунок 49. Модели машинного обучения

Каждая модель формирует свой вердикт по ссылке, который отображается на шкале с обозначением уровня опасности в процентном отношении.

Этапы проверки ссылки на фишинг машинным обучением:

– Получение первичной информации о ресурсе (доступность ресурса, владелец домена и т.д.)

– Анализ ссылки на подозрительность написания с использованием ансамбля нейросетевых трансформеров NLP:

a. анализ, насколько ссылка является подозрительной

b. анализ на тайпсквоттинг (намеренные опечатки и мимикрия под бренд), например, «amaz0n»

c. анализ на киберсквоттинг (использование известного доменного имени в другой зоне), например, yandex.ru → yandex.com

– Глубокий анализ страницы ансамблем моделей (около 800 анализируемых признаков: контент станицы, код страницы, скрипты, ключевые слова, скрытые элементы, рейтинг, дата регистрации и проч.)

– Эвристический анализ веб-ресурса по мере получения информации о сайте

– Визуальный анализ сайта (подозрительность сайта, его контент):

a. структурное сравнение скриншота со скриншотами в базе наиболее популярных атак

b. поиск элементов (логотипы, формы оплаты, формы ввода)

c. выделение текста и анализ контента страницы для выделения категории эвристики

d. сравнение текста, который показывается пользователю, и который скрыт в коде

e. поиск ключевых слов-маркеров

Для получения признаков модулей машинного обучения для системы KAIROS дополнительно осуществляется автоматический сбор информации в источниках фишинговых ресурсов:

- Позиция в рейтинге alexa (при отсутствии в локальной базе данных) [http://data.alexa.com];
- Индексация в Google [http://google.com];
- Наличие в интернет архиве [http://web.archive.org];
- Информация о домене WHOIS [https://www.whois.com];
- Исследуемый ресурс, перенаправления URL (англ., redirect) и JS скрипты из тела страницы.

Также в распоряжении моделей ML находятся внутренние базы данных фишинговых ресурсов:

- Рейтинг Alexa,
- Рейтинг PageRank,
- Базы данных вредоносных хешей системы KAIROS.

Дообучение моделей ML производится в том числе за счет ботов, которые осуществляют регулярный сбор информации о вредоносных ссылках во внешних источниках:

- [https://openphish.com/],
- [https://phishtank.com],
- [https:// feodotracker.abuse.ch],
- [https:// cybercrime-tracker.net],
- [https:// urlhaus.abuse.ch],
- [https://raw.githubusercontent.com],
- [https://telegram.org/], тематические Телеграм-каналы.

Боты устанавливаются на стенде заказчика и обогащают его локальную базу.

Для добавления нового Телеграм-канала (для прослушивания ботом), следует, в разделе «Настройки» – «Серверы» – «Панель управления ботами», войти в меню редактирования бота «bot_listen_telegram» при помощи иконки «Настройки» напротив него.- **Затем, в поле «Входные каналы» , добавить новый Телеграм**-канал и сохранить изменения (Рисунок 50).

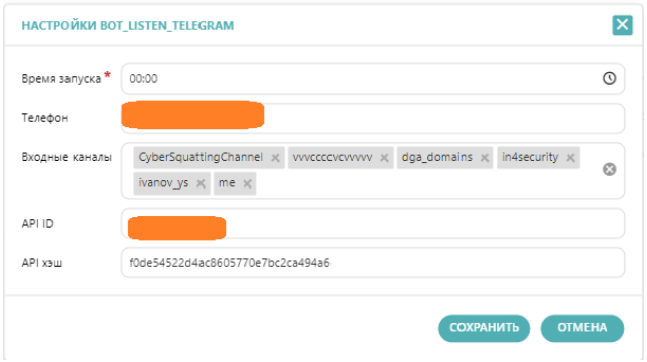

Рисунок 50. Форма редактирования бота

8.4 Анализ во внешних аналитических сервисах

Внешние аналитические сервисы осуществляют проверку цепочки переходов по веб-ссылкам с основной ссылки, проверяемой в системе. Система направляет ссылку параллельно на анализ и проверку во внешних базах данных следующих источников:

– XSEO [http://xseo.in]

– PhishTank [http://phishtank.org]

– UrlScan [https://urlscan.io]

– VirusTotal Domain [https://www.virustotal.com/]

– VirusTotal URL [https://www.virustotal.com/].

При получении ссылки на проверку происходит вычисление хеш отпечатка для домена и для всей ссылки по алгоритму sha256.

При проверке ссылки или домена во внешних системах, происходит GET запрос на API внешнего сервиса с передачей ТОЛЬКО хеш отпечатка

Например, для Virus Total, происходит GET запрос вида:

https://www.virustotal.com/ui/urls/<hash>

где hash – вычисленный хеш отпечаток объекта.

В случае, если хэш объекта найден в БД VirusTotal, возвращается подробный отчет.

Аналогичные запросы с передачей хеш отпечатка выполняются для остальных внешних ресурсов.

При необходимости, обращение к внешним аналитическим ресурсам может быть полностью выключено. Для этого необходимо выполнить 2 настройки:

1) В разделе: Настройки – Исследования – Ресурсы внешнего анализа (Рисунок 51)

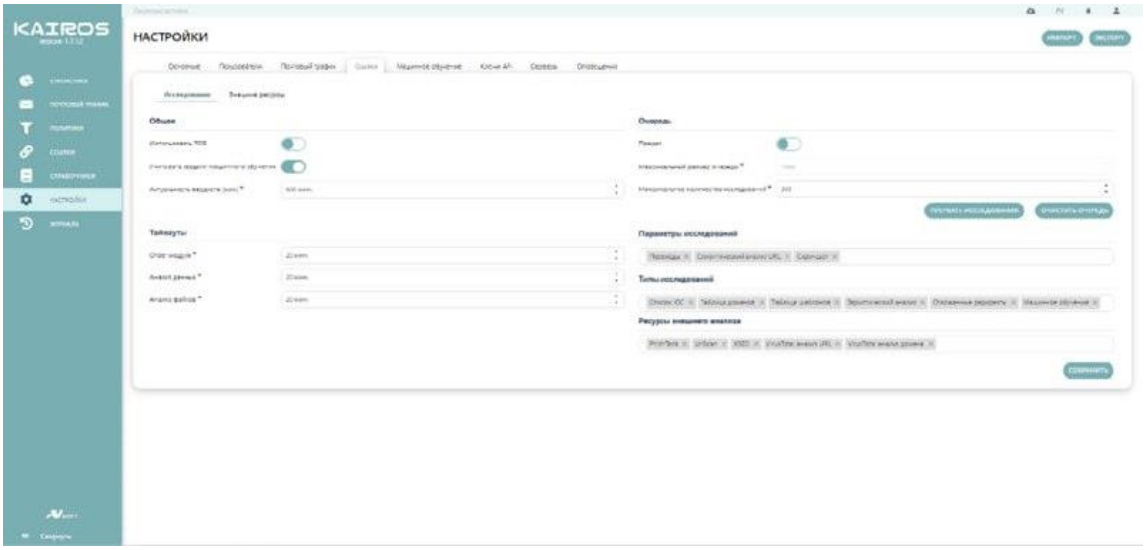

Рисунок 51. Отключение обращения к внешним ресурсам

Необходимо выключить соответствующие Ресурсы внешнего анализа

При таком режиме вердикт будет выноситься только модулями машинного обучения и внутренними репутационными базами

2) Для выключения получения аналитической информации о домене, необходимо перейти в раздел: Настройки – Серверы – Модуль проверки ссылок – Настройки узла линкчекера

После чего снять флаг с параметра «Получение информации о домене» (Рисунок 52)

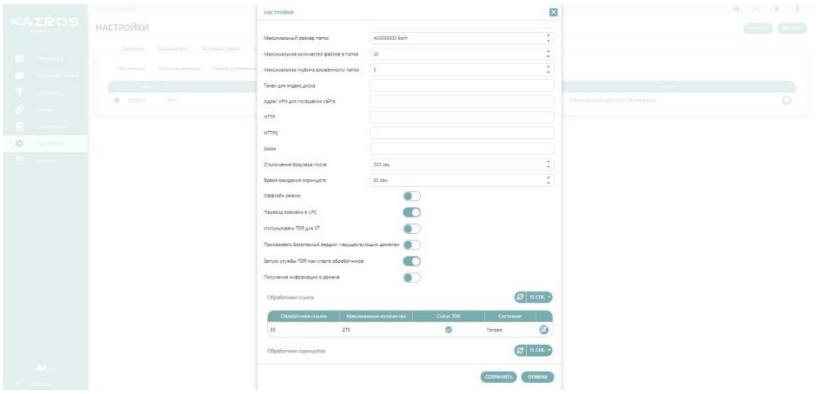

Рисунок 52. Выключение получения аналитической информации о домене

После выполнения обоих процедур модуль проверки ссылок не будет использовать внешние ресурсы для анализа.

По результатам анализа каждый внешний аналитический сервис формирует ссылке вердикт.

Вердикт, формируемый ссылке источником VirusTotal, состоит из вердиктов доверенных и недоверенных антивирусов, входящих в состав VirusTotal. Ознакомиться с вердиктами всех антивирусов можно, нажав на интерактивное название VirusTotal Domain или VirusTotal URL в отчете по исследованию ссылки (Рисунок 53).

Сервисы проверки ссылок	Доверенный	Вердикт
alphaMountain.ai	Доверенный	Вредоносный
Fortinet	Доверенный	Вредоносный
G-Data	Доверенный	Вредоносный
Forcepoint ThreatSeeker	Доверенный	Подозрительный
Avira	Доверенный	Безопасный
Bfore.Ai PreCrime	Доверенный	Безопасный
Cyan	Доверенный	Безопасный
CyRadar	Доверенный	Безопасный
DNS8	Доверенный	Безопасный
Dr.Web	Доверенный	Безопасный
ESET	Доверенный	Безопасный
K7AntiVirus	Доверенный	Безопасный
Netcraft	Доверенный	Безопасный
Scantitan	Доверенный	Безопасный
Segasec	Доверенный	Безопасный
StopForumSpam	Доверенный	Безопасный
zvelo	Доверенный	Безопасный
BitDefender	Недоверенный	Вредоносный
CRDF	Недоверенный	Вредоносный
Heimdal Security	Недоверенный	Вредоносный
Kaspersky	Недоверенный	Вредоносный
Seclookup	Недоверенный	Вредоносный
Sophos	Недоверенный	Вредоносный
Viettel Threat Intelligence	Недоверенный	Вредоносный
Webroot	Недоверенный	Вредоносный

Рисунок 53. Список антивирусов VirusTotal (фрагмент)

При учете вердикта, формируемого ссылке источником VirusTotal, в интерфейсе Системы применяются тонкие настройки. В разделе «Настройки» - «Ссылки» - «Внешние ресурсы» доступен список доверенных антивирусов в составе VirusTotal (Рисунок 54).

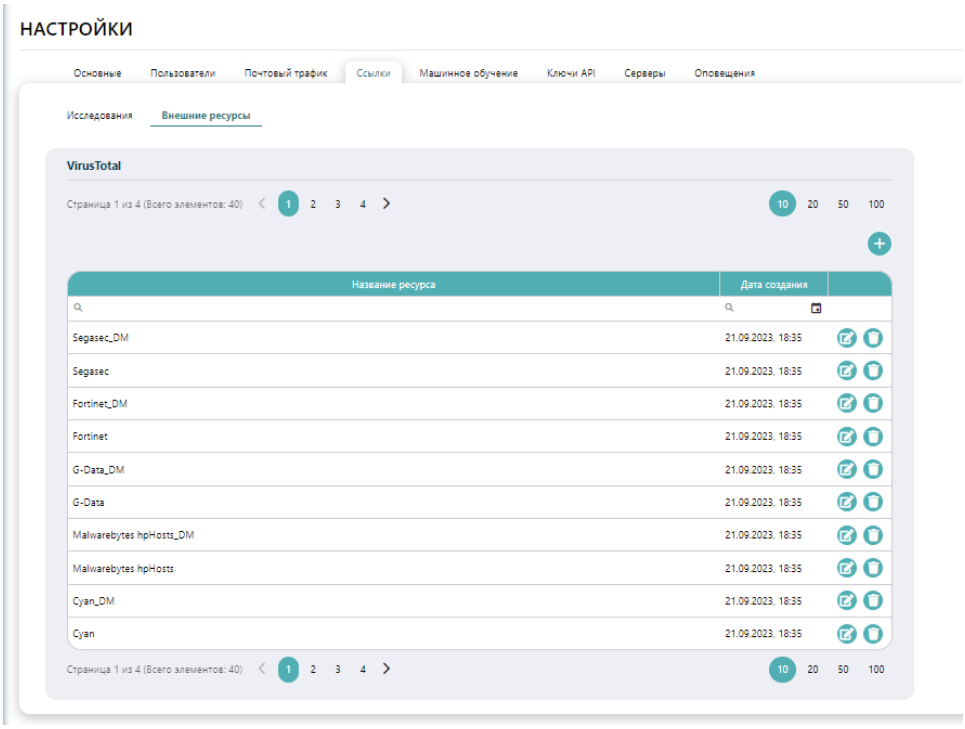

Рисунок 54. Настройка учета вердикта от VirusTotal

Вердикт, сформированный ссылке доверенным антивирусом, учитывается в системе. Список доверенных антивирусов является рекомендованным, с возможностью добавления или удаления антивирусов. Все остальные антивирусы, не перечисленные в списке доверенных антивирусов, являются недоверенными. Вердикт, сформированный ссылке антивирусом, не учитывается в системе.

Для уменьшения числа ложных срабатываний, в системе предусмотрена возможность настройки порога учета вердикта недоверенных антивирусов. В предустановленном варианте порог учета вердикта антивирусов равен десяти. Это означает, что, если вредоносный вердикт ссылке сформирован десятью или более недоверенными антивирусами VirusTotal, вердикт будет учитываться системой наравне с вердиктом доверенных антивирусов.

После внесения изменений в предустановленные настройки, для их сохранения в системе, необходимо нажать на кнопку «Сохранить».

Итоговый вердикт ссылки по результатам исследования формируется на основании наивысшего по вредоносности из вердиктов, присваиваемых модулями анализа ссылки.

9 Раздел «Справочники»

В разделе «Справочники» - «Системные» - «Ссылки» - «Домены» приведены перечни доменов и шаблонов регулярных выражений, к которым обращается система при исследовании ссылки (Рисунок 55).

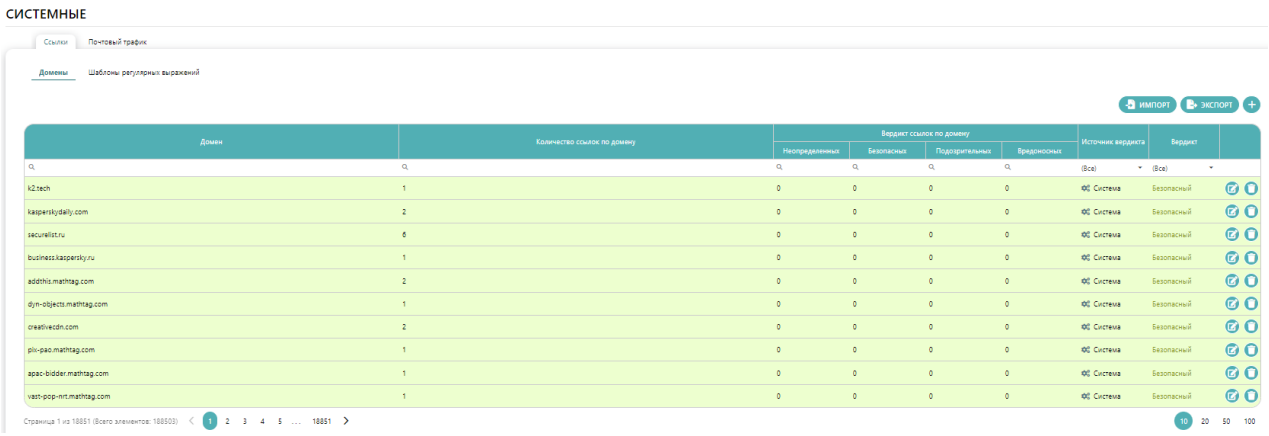

Рисунок 55. Раздел «Справочники» - «Системные»

Данные справочники могут быть дополнены вручную при помощи иконки «Добавить» (Рисунок 56).

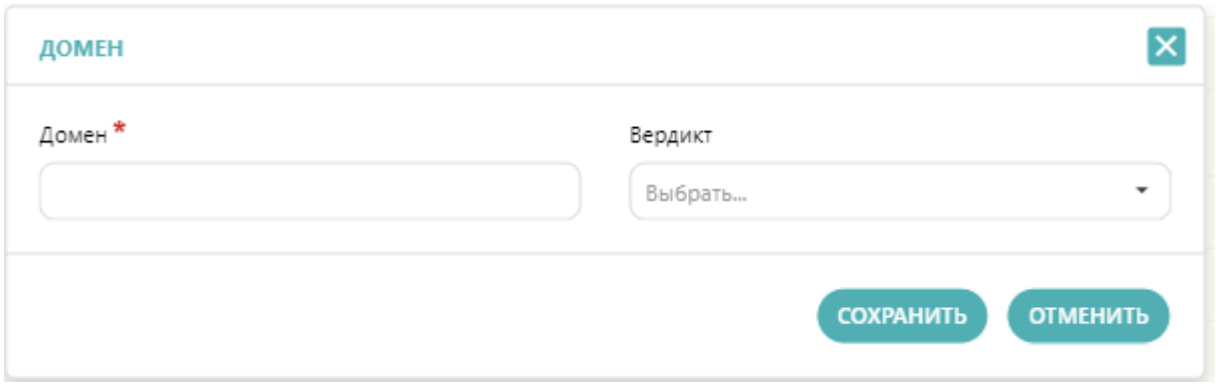

Рисунок 56. Форма добавления домена

В разделе «Шаблоны регулярных выражений» находятся шаблоны URL и группы шаблонов. (Рисунок 57). Для добавления нужно нажать кнопку «Добавить» и заполнить поля.

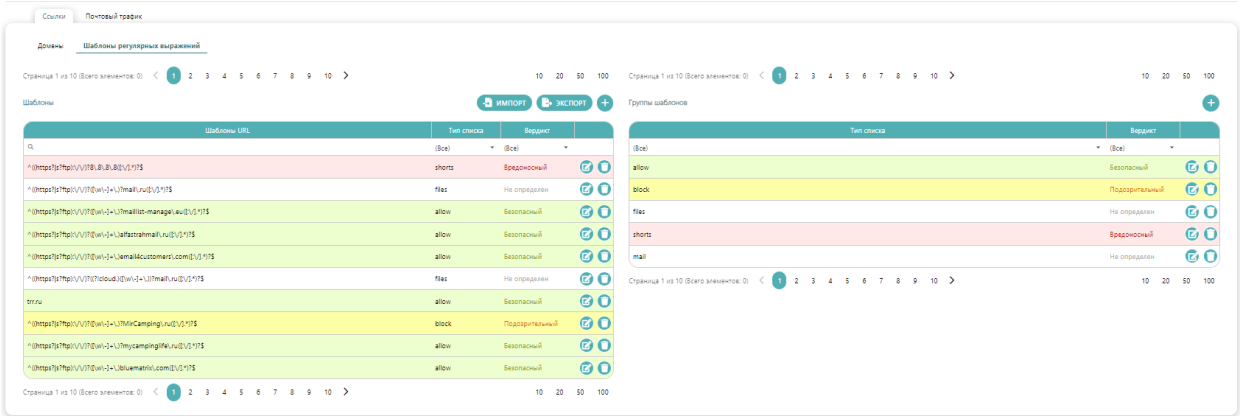

Рисунок 57. Шаблоны регулярных выражений

В разделе «Справочники» - «Системные» во вкладке «Почтовый трафик» отображается белый список почтовых клиентов (Рисунок 58).

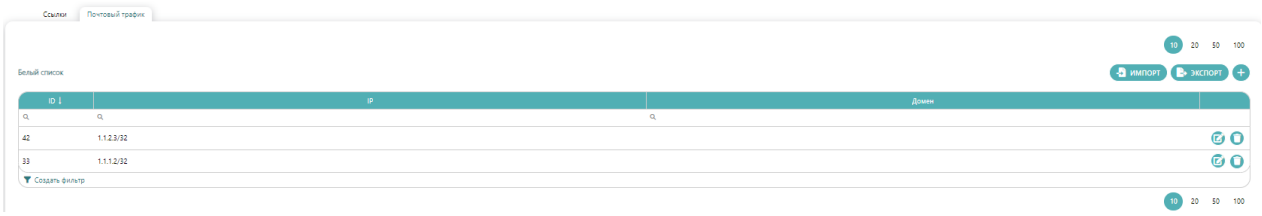

Рисунок 58. Список почтовых клиентов

Данный раздел может быть дополнен вручную при помощи иконки «Добавить» (Рисунок 59).

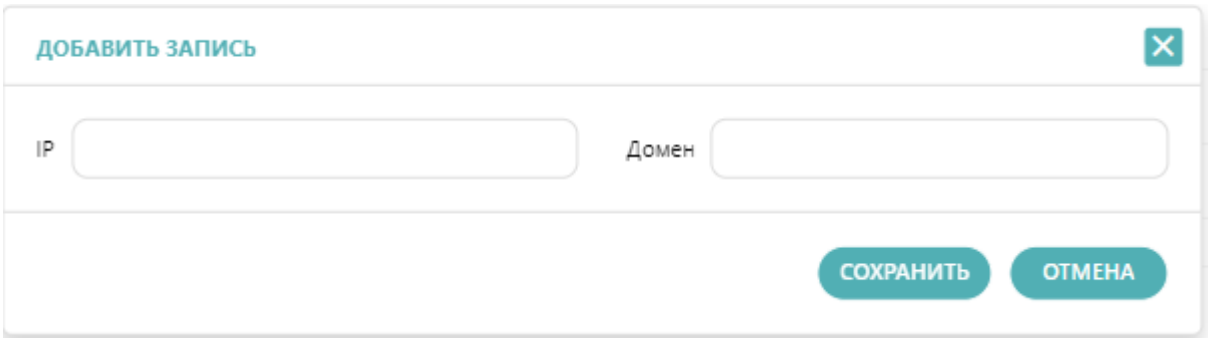

Рисунок 59. Форма добавления почтовых клиентов

В разделе «Справочники» – «Аналитика» приведены аналитические ресурсы, списки почтовых клиентов и стран, которые участвуют в анализе почтовых заголовков и ссылок. Во вкладке «Почтовый трафик» перечислены индикаторы почтовых заголовков для проверки наличия в них признаков спама, фишинга или других подозрительных действий, каждый из который можно индивидуально включить или исключить при проверке письма. Так же вкладка имеет белый список почтовых клиентов, перечень одноразовых почтовых ящиков и черный список стран (Рисунок 60).

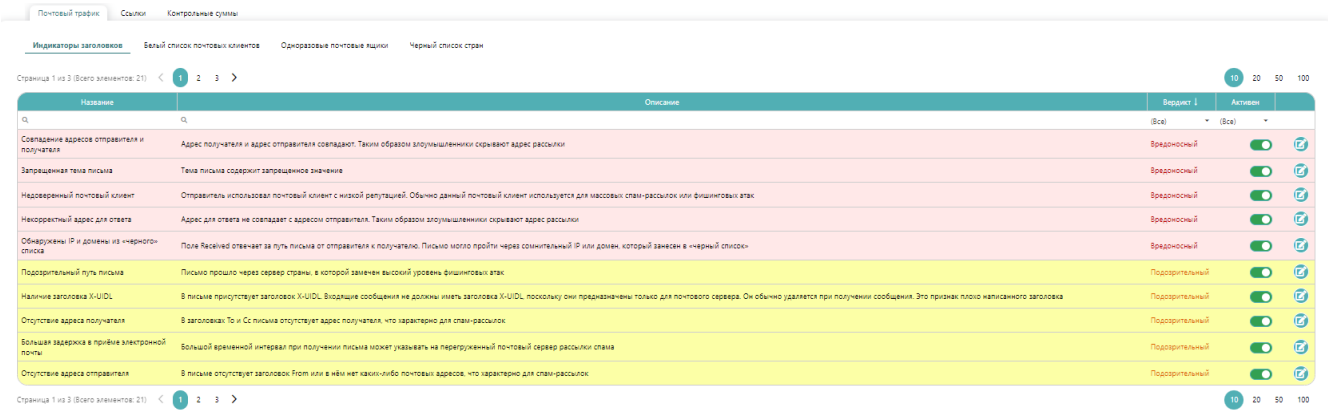

Рисунок 60. Раздел «Справочники» - «Аналитика»

Каждый из индикаторов почтовых заголовков обладает вредоносным или подозрительным вердиктом, а также флаг «Активен». Для отключения работы индикатора следует выключить флаг в столбце «Активен». Вердикт

индикатора можно изменить, нажав на иконку «Редактировать» напротив нужного индикатора (Рисунок 61).

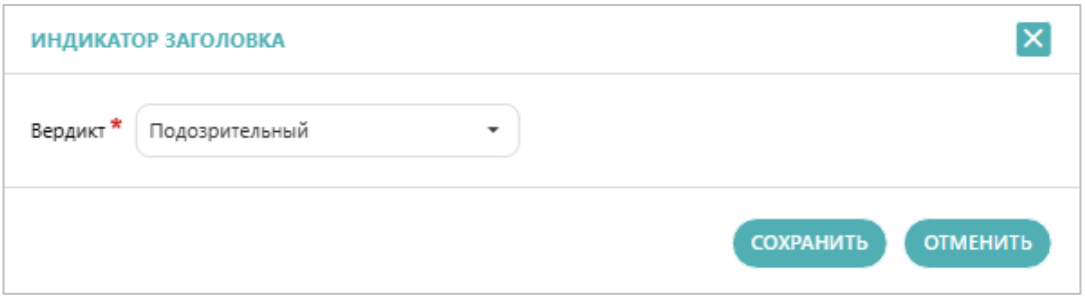

Рисунок 61. Редактирование индикатора

В открывшейся форме следует указать новый вердикт индикатора. После внесения изменений надо нажать кнопку «Сохранить» и убедиться, что изменения отобразились в интерфейсе таблицы индикаторов.

Для системных индикаторов, перечисленных во вкладке «Ссылки» и использующихся для пояснения сформированного вердикта ссылке, также предусмотрена возможность изменения вердикта и отключения работы индикатора через иконку «Редактировать» (Рисунок 62).

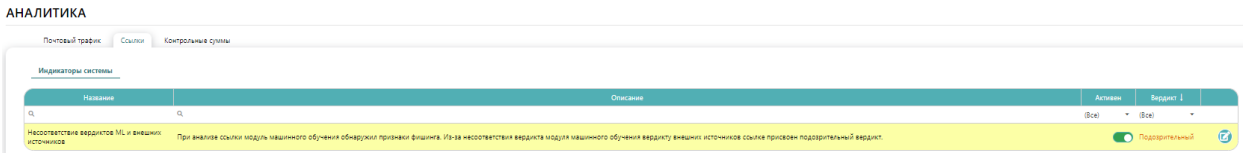

Рисунок 62. Список системных индикаторов

В разделе «Справочники» - «Аналитика» есть вкладка «Белый список почтовых клиентов», в которой отображаются пользователи, которые не проходят проверку (Рисунок 63)

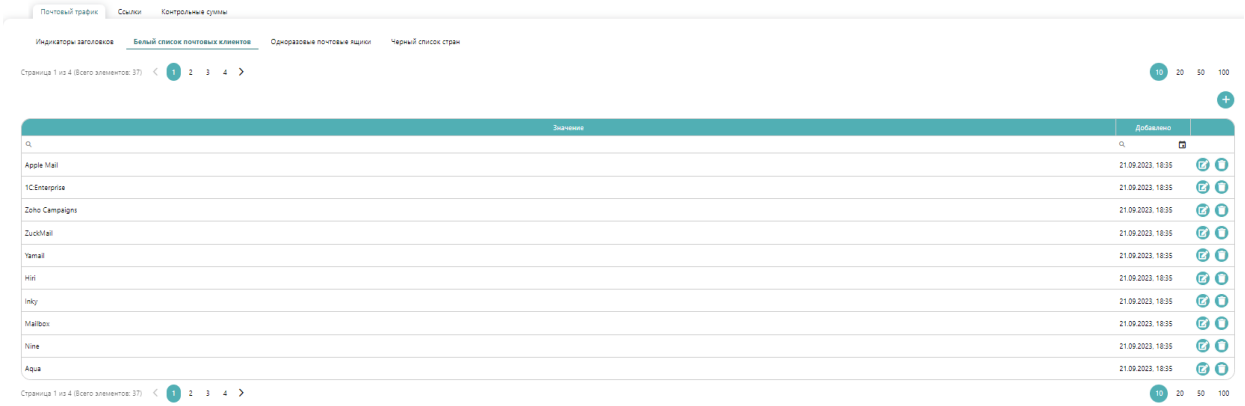

Рисунок 63. Белый список почтовых клиентов

Во вкладке «Одноразовые почтовые ящики» отображаются адреса почты, которые использовались один раз (Рисунок 64)

Одноразовые почтовые ящики могут использоваться пользователями для регистрации где-либо, и система не будет их повреждать при переходе по ссылке (т.к. по ней только 1 раз можно перейти)

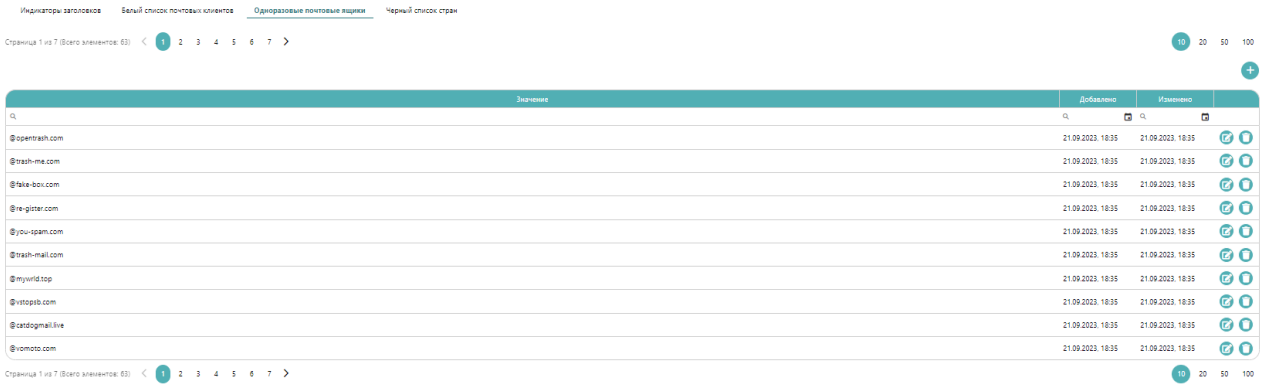

Рисунок 64. Одноразовые почтовые ящики

Во вкладке «Чёрный список стран» находятся страны, от которых не будет приходить почта (Рисунок 65)

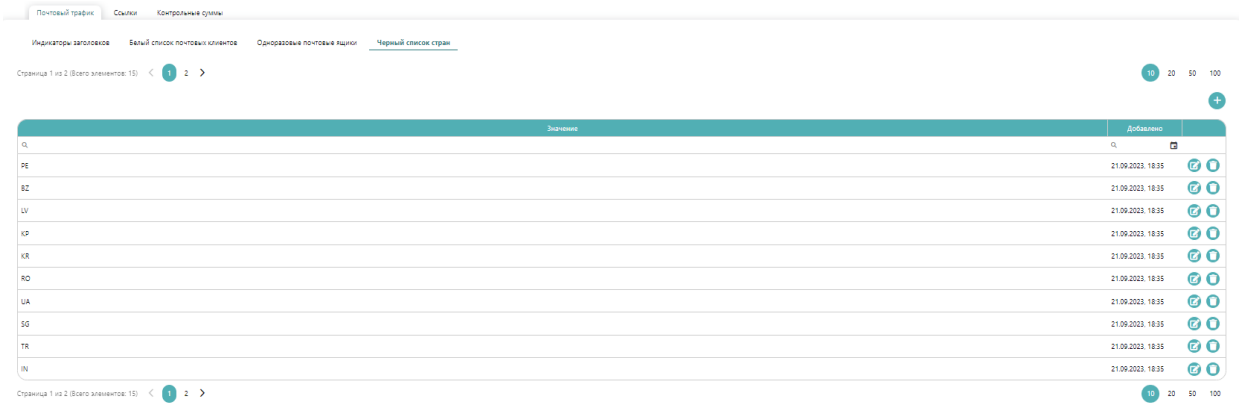

Рисунок 65. Черный список стран