



AVSOFT KAIROS

Система защиты от спама и фишинга

Руководство пользователя

**Москва
2022г.**

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

ООО «АВ Софт»

www.avsw.ru

© 2010-2022 ООО «АВ Софт»

Версия документа

Руководство пользователя v1.1

Июнь 11, 2022.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

Документ может быть изменен без предварительного уведомления.

СОДЕРЖАНИЕ

1	Термины и определения	4
2	Перечень сокращений.....	5
3	Назначение программы	6
4	Авторизация и элементы управления	6
4.1	Авторизация в системе	6
4.2	Элементы управления веб-интерфейсом.....	7
5	Раздел «Статистика»	10
6	Раздел «Безопасность».....	10
6.1	Отчет по антиспам проверке.....	10
6.2	Блок проверки письма на спам	12
6.3	Блок проверки машинного обучения	13
7	Раздел «Источники».....	14
7.1	Отчет по почтовому трафику.....	14
7.2	Анализ почтовых заголовков.....	16
8	Раздел «Ссылки»	18
8.1	Ручной режим исследования ссылки	18
8.2	Отчет по ссылке	19
9	Раздел «Исследования»	21
10	Раздел «Настройки»	24
11	Раздел «Журналы»	24

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.	SPF	Метод, используемый для верификации серверов в домене отправителя, с помощью их перечисления в txt-записи DNS-запроса
6.	SS	Набор правил для фильтрации спама, которые анализируют тело и заголовок письма. Также использует DKIM и SPF.
7.	ML	Модели машинного обучения анализируют письма на принадлежность к спаму и ссылки на принадлежность к фишингу

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.	DKIM	DomainKeys Identified Mail
3.	DMARC	Domain-based Message Authentication, Reporting and Conformance
4.	DNS	Domain Name System
5.	CPU	Central Processing Unit
6.	HTTP	Hypertext Transfer Protocol
7.	HTTPS	Hypertext Transfer Protocol Secure
8.	ML	Machine Learning
9.	SS	Spam Score
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 (далее – система KAIROS) предназначена для комплексного обнаружения и фильтрации спама, а также фишингового контента в реальном времени.

4 Авторизация и элементы управления

4.1 Авторизация в системе

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

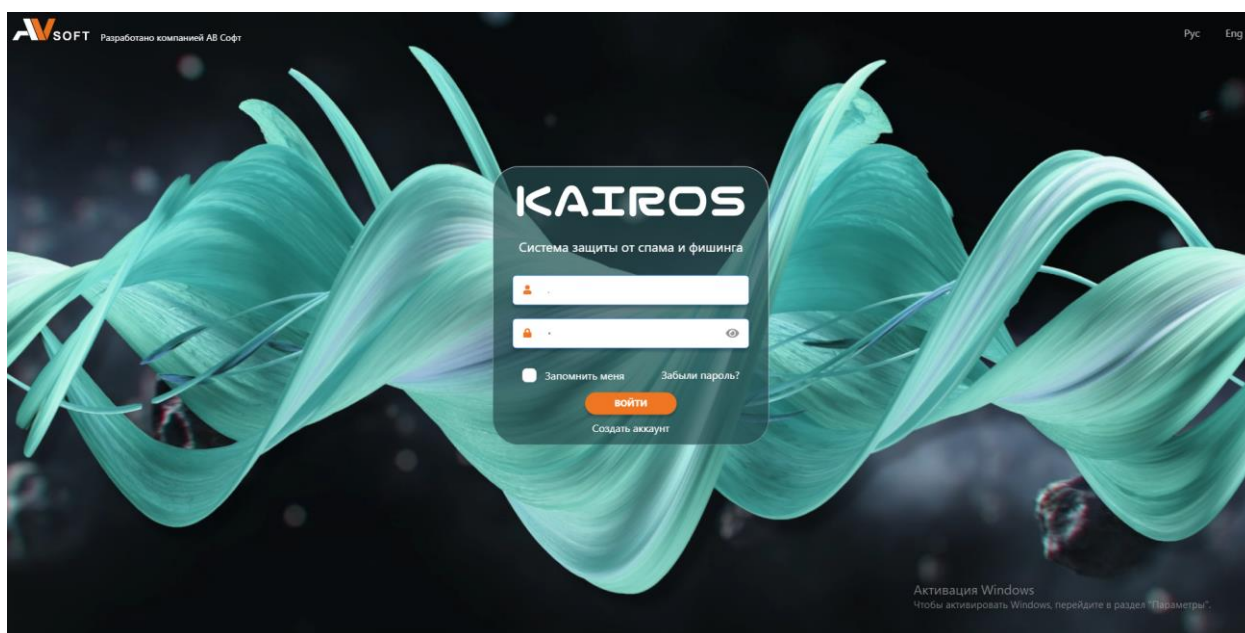


Рисунок 1. Страница авторизации пользователя в системе KAIROS

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

Таблица 3. Описание функциональных разделов в системе





№	Раздел	Описание
1.	Статистика	Содержит статистическую информацию.
2.	Безопасность	Содержит информацию о всех письмах, поступающих в систему и результате их проверки на спам.

№	Раздел	Описание
3.	Источники / Почтовый трафик	Содержит информацию о письмах, прошедших антиспам проверку, и результате их проверки на фишинг.
4.	Ссылки	Содержит информацию по всем веб-ссылкам, исследованным в системе.
5.	Исследования	Содержит информацию по всем исследованиям, проводимым в системе.
6.	Настройки	Содержит настройки по всем компонентам системы.
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 KAIROS представлены в таблице 4.

Таблица 4. Элементы управления интерфейсом

№	Элемент	Назначение	Изображение
1.	Кнопка «Загрузка ссылки»	Выполняет загрузку ссылки 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 каких-либо уведомлениях	

№	Элемент	Назначение	Изображение
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	
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	

№	Элемент	Назначение	Изображение
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	
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.

5 Раздел «Статистика»

В разделе «Статистика» представлены диаграммы со статистическими данными по вердиктам проанализированных ссылок и источникам их поступления в систему (Рисунок 2).



Рисунок 2. Раздел «Статистика»

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. В таблице «Вредоносные ссылки» отображаются последние выявленные системой вредоносные веб-ссылки. В таблице присутствует активная кнопка «Отчёт» при нажатии на которую происходит переход в отчет по веб-ссылке.

6 Раздел «Безопасность»

6.1 Отчет по антиспам проверке

В разделе «Безопасность» содержится информация по всем письмам, поступающим в систему KAIROS, которые проходят проверку на антиспам (Рисунок 3).

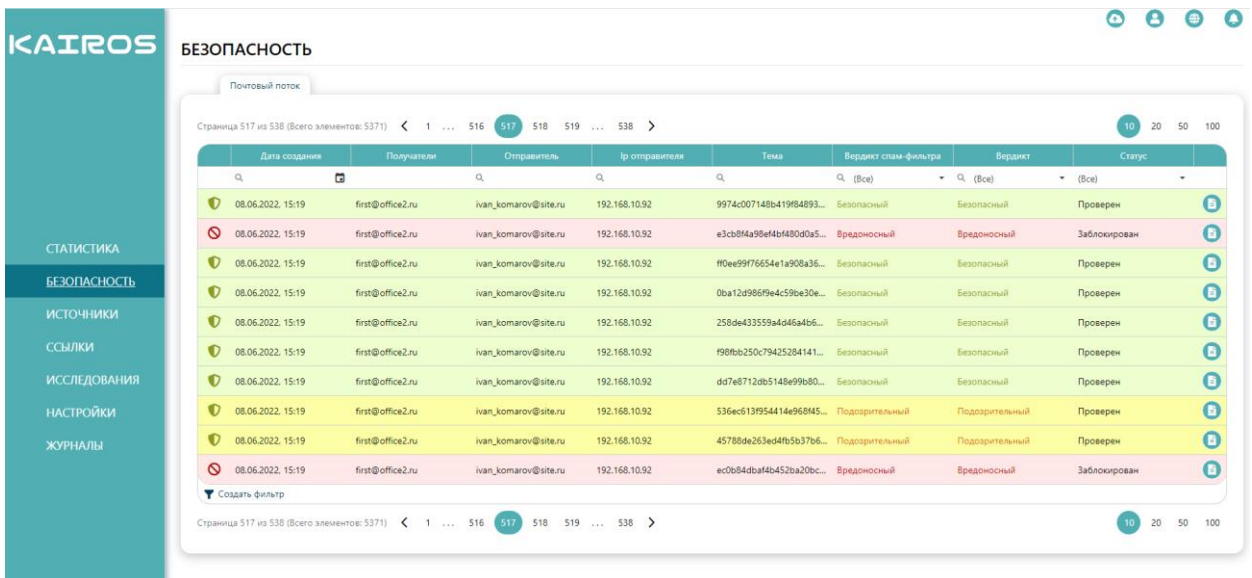


Рисунок 3. Раздел «Безопасность»

Результатом проверки письма на наличие спама является вердикт письма. Обоснованием вердикта является отчет по антиспам проверке. Отчет доступен при нажатии на иконку «Отчет» напротив письма в разделе «Безопасность» (Рисунок 4).

ОТЧЕТ ПО АНТИСПАМ ПРОВЕРКЕ

ВРЕДОНОСНЫЙ

Общая информация

Отправитель	ivan_komarov@site.ru	Получатели	first@office2.ru
Тема	2d2cb3aa47734ce7b59c198dc...	ID	8265
Доставлено	Да	Состояние	Заблокирован
Время исследования	10.06.2022, 20:06:07.000 - 20:07:25.000 (1 мин. 18 сек.)		

ДЕЙСТВИЯ

Антиспам

- DKIM
 Безопасный
- DMARK
 Безопасный
- SPF
 Безопасный
- SA
 Вредоносный
- Спам
 Вредоносный

ML

Спам	100%
Теги	
Категории	

Рисунок 4. Отчет по антиспам проверке

Отчет содержит:

- блок общей информации по письму,
- блок проверки на наличие спама,
- блок проверки машинного обучения.

В блоке общей информации содержатся данные по отправителю, получателю письма, тема письма, его ID и его статус по результатам проверки.

6.2 Блок проверки письма на спам

Блок проверки на спам содержит вердикты, сформированные различными модулями и политиками проверки письма на антиспам: DKIM, DMARK, SPF, SS.

Технология DomainKeys Identified Mail (DKIM) отмечает исходящую почту зашифрованной подписью внутри заголовков, 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 со значением “pass”, если ЭЦП корректна, или значениями “fail” / “none”, если ЭЦП не прошла проверку. Безопасный вердикт соответствует значению почтового заголовка “dkim=pass”.

Технология Domain-based Message Authentication, Reporting and Conformance (DMARC) проверяет репутацию почтовых сервисов и интернет-провайдеров. При прохождении письмом DMARC проверки, “dmarc=pass”, оно получает безопасный вердикт.

Метод Sender Policy Framework (SPF) подтверждает, что сообщения с конкретного домена были отправлены с сервера, который контролируется владельцем этого домена. Если проверка письмом пройдена, SPF формирует заголовок со значением “pass”, в остальных случаях заголовок может принимать другие значения (“fail”, “softfail”, “neutral”, “none”, “temperror”, “permerror”). Безопасный вердикт соответствует значению почтового заголовка “spf=pass”.

Почтовый фильтр Spam Score выявляет спам путем проведения эвристических проверок почтовых заголовков и текстов. Результатом работы фильтра является расчет коэффициента. При превышении коэффициентом установленного порога спама, письмо получает подозрительный или вредоносный вердикт.

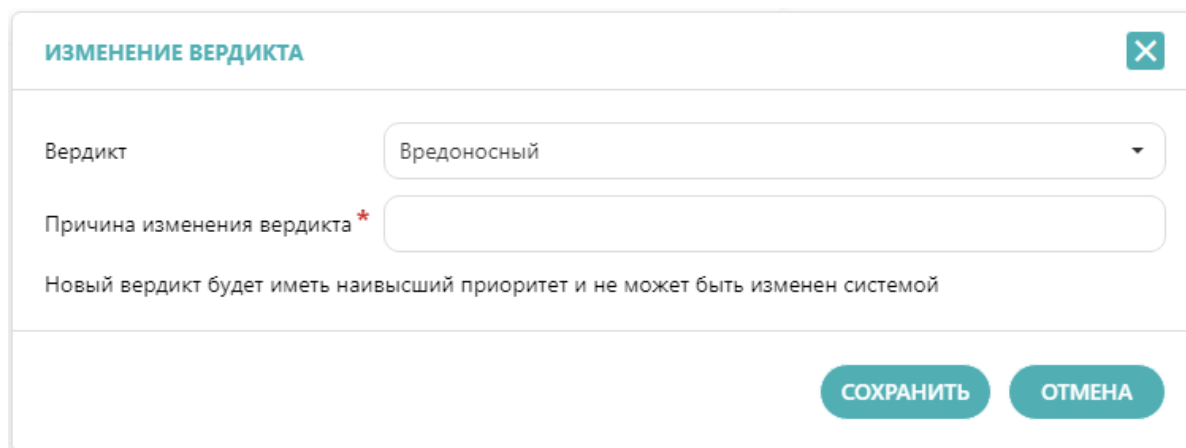
6.3 Блок проверки машинного обучения

Блок машинного обучения содержит результат проверки на спам в процентном выражении 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 этих целей используются две модели. Первая - табличная модель CatBoost, которая анализирует извлеченный из письма эмбединг и классифицирует его по двум категориям: Спам / Не спам. Вторая модель, с использованием методов полу-контролируемого обучения, определяет категорию контента письма (рассылка, знакомства, деловая переписка и т.д.). Всего модель использует более 55 различных категорий. На основании выявленных категорий письму присваиваются соответствующие теги в системе.

Итоговый вердикт письма по результатам проверки на спам формируется на основе наивысшего по вредоносности вердикта модулей.

Вердикт отчета по антиспам проверке может быть принудительно изменен в ручном режиме. Для этого надо нажать на кнопку «Действия» в интерфейсе отчета (Рисунок 5).



ИЗМЕНЕНИЕ ВЕРДИКТА

Вердикт Вредоносный

Причина изменения вердикта *

Новый вердикт будет иметь наивысший приоритет и не может быть изменен системой

СОХРАНИТЬ ОТМЕНА

Рисунок 5. 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.

7 Раздел «Источники»

7.1 Отчет по почтовому трафику

Во вкладке «Почтовый трафик» раздела «Источники» содержится информация по всем письмам, имеющим ссылки, которые проходят проверку в системе на фишинг (Рисунок 6).

ID	Дата	Получатель	Отправитель	Тема	Вложений	Ссылок	Статус	Вердикт
20808	01.06.2022. 18:08	first@office2.ru	sergei_komarov@site.ru	Презентация	0	1	Завершено	Безопасный
20807	01.06.2022. 18:06	first@office2.ru	sergei_komarov@site.ru	Счет на оплату NR228094117970...	0	1	Завершено	Безопасный
20806	01.06.2022. 18:05	first@office2.ru	sergei_komarov@site.ru	Согласие оппонента. Диссертац...	0	3	Завершено	Безопасный
20805	01.06.2022. 18:04	first@office2.ru	sergei_komarov@site.ru	*****	0	1	Завершено	Безопасный
20804	01.06.2022. 17:57	first@office2.ru	sergei_komarov@site.ru	Напоминание о поездке!	0	1	Завершено	Подозрительный
20803	01.06.2022. 17:37	first@office2.ru	sergei_komarov@site.ru	Напоминание о поездке!	0	1	Завершено	Подозрительный
20802	01.06.2022. 17:28	first@office2.ru	sergei_komarov@site.ru	Attn : Your PayPal account access ...	0	1	Завершено	Безопасный
20801	01.06.2022. 17:26	first@office2.ru	sergei_komarov@site.ru	Follow up - Fuzzy Control Systems	0	5	Завершено	Безопасный
20800	01.06.2022. 17:26	first@office2.ru	sergei_komarov@site.ru	Special Issue on "Automotive Eng...	0	2	Завершено	Безопасный
20799	01.06.2022. 17:24	first@office2.ru	sergei_komarov@site.ru	Заявка 661443 от 18.05.2022	0	1	Завершено	Вредоносный

Рисунок 6. Вкладка «Почтовый трафик»

Результатом проверки письма является отчет по почтовому трафику. Просмотреть отчет можно, нажав на иконку «Отчет» напротив письма во вкладке «Почтовый трафик» (Рисунок 7).

Ссылка	Контрольная сумма (SHA-256)	Статус	Вердикт
http://mail.amazon.com/.../signin?openid.pape_max_auth_age=0&openid.return_to=https	9709bfe39d25beda098bc8a280dc8d5f9b203e814591194f4850c3d...	Проверена	Вредоносный
https://aef.global/tain/upsms/users/Login.ID-26142	3fa99cbb680329cab27a3b156b9a968fe0358feb8c2aee32b675c25f9...	Проверена	Вредоносный
specs.openid.net/auth/2.0	88e369c09f335e7734a9d9b726dfc831c280a2bc967b4348545d5c4...	Проверена	Безопасный
specs.openid.net/auth/2.0/identifier_select&openid.assoc_handle=a...	481c90a580723c17906b49f41ca4a991188e0ec490b9442ae438a782c...	Проверена	Безопасный
specs.openid.net/auth/2.0/identifier_select&openid.ns=http	65212b046977696e6e94a86-956b7978a8505d9a362aee2de69b0a...	Проверена	Безопасный
www.amazon.com/?_encoding=utf8&ref_namv_hdr_signin&openid.identity=http	8b2e3a9b7b93b108088274b4a5eb5c166276bc57bb00314e8043d6e...	Проверена	Безопасный

Рисунок 7. Отчет по почтовому трафику, вкладка «Ссылки»

В отчете по проверке письма отображается:

- идентифицирующая информация по письму,
- информация по заголовкам электронного письма,
- результаты проверки ссылок, обнаруженных в письме.

После прохождения письмом проверки на спам в разделе «Безопасность», производится его анализ на фишинг по двум направлениям:

- анализ ссылок, указанных в письме, на принадлежность к фишинговым ресурсам
- анализ метаданных почтового заголовка.

Результат анализа каждого из направлений отображается в отдельной вкладке в отчете по почтовому трафику.

Каждый из обнаруженных объектов анализа (ссылка) направляется на исследование системой KAIROS и, в зависимости от его вредоносности, получает вердикт: безопасный, подозрительный или вредоносный. Результат исследования ссылки, обосновывающий ее вердикт, можно посмотреть, пройдя по интерактивной иконке отчета напротив ссылки.

При обнаружении в письме подозрительного или вредоносного объекта, вкладка отчета по почтовому трафику будет окрашена в соответствующий цвет: желтый или красный. Итоговый вердикт электронного письма формируется на основании наивысшего по вредоносности вердикта его объектов.

В формировании вердикта письма также принимает участие вердикт, присваиваемый его заголовку. Анализ метаданных почтового заголовка осуществляется индикаторами заголовков системы KAIROS. Каждый из индикаторов направлен на проверку определенного почтового заголовка. При обнаружении подозрительных или вредоносных данных в заголовке письма в отчете по почтовому трафику отображается сработавший индикатор и его описание (Рисунок 8).

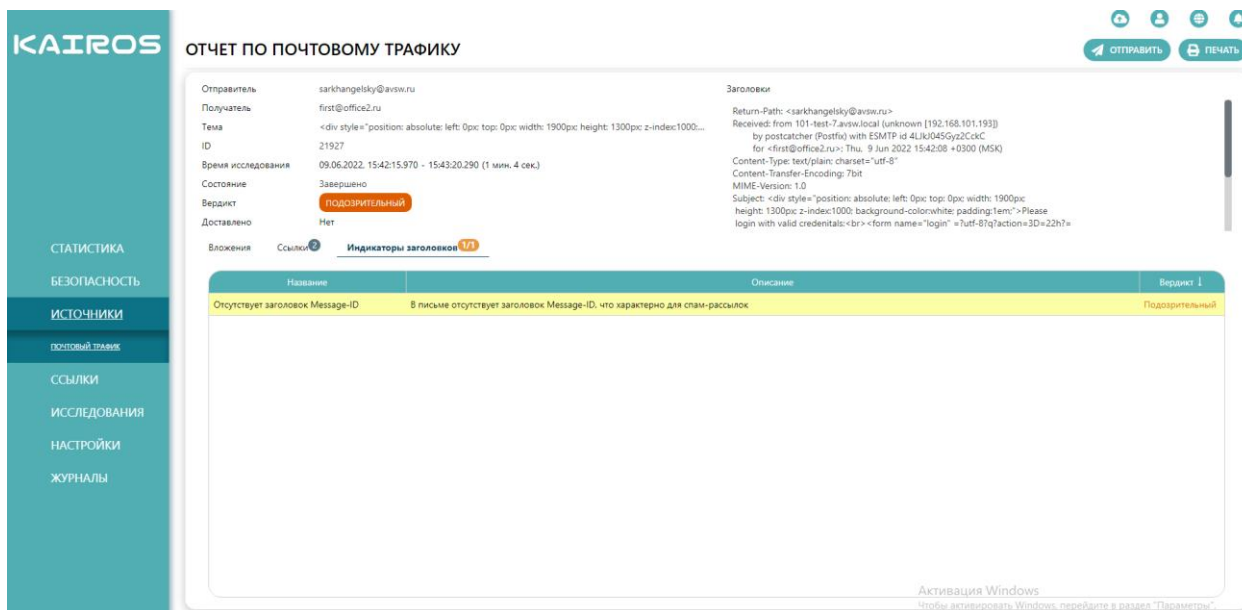


Рисунок 8. Отчет по почтовому трафику, вкладка «Индикаторы заголовков»

7.2 Анализ почтовых заголовков

Перечень почтовых заголовков и результат их анализа представлен в таблице 5.

Таблица 5. Анализ почтовых заголовков

Почтовый заголовок	Значение заголовка	Индикатор	Описание
X-Distribution	bulk	Наличие заголовка X-Distribution со значением bulk	Письмо адресовано большому количеству получателей. Присутствие данного заголовка чаще всего свидетельствует о спам-рассылках.
Всс	Есть данные	Наличие заголовка Всс	Заголовок скрытой копии. Это признак плохо написанного заголовка. Заголовок Всс 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

Почтовый заголовок	Значение заголовка	Индикатор	Описание
			обычно удаляется при получении сообщения. Это признак плохо написанного заголовка.
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»,

Почтовый заголовок	Значение заголовка	Индикатор	Описание
			это значит, что злоумышленники скрывают адрес рассылки.
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

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 «Загрузка ссылки» 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 9).

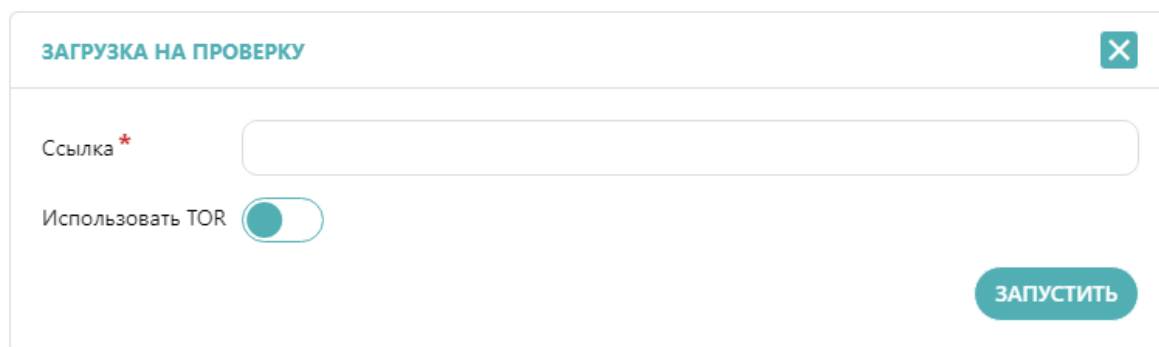


Рисунок 9. Форма загрузки ссылки

При выборе способа загрузки ссылки при помощи кнопки «Создать» в разделе «Исследования» отобразится форма «Создание исследования ссылки», в которую следует вставить проверяемую ссылку и указать в поле «Тип исследования ссылки» используемые в проверке модули. По окончании ввода данных необходимо нажать кнопку «Запустить». (Рисунок 10).

СОЗДАНИЕ ИССЛЕДОВАНИЯ ССЫЛКИ

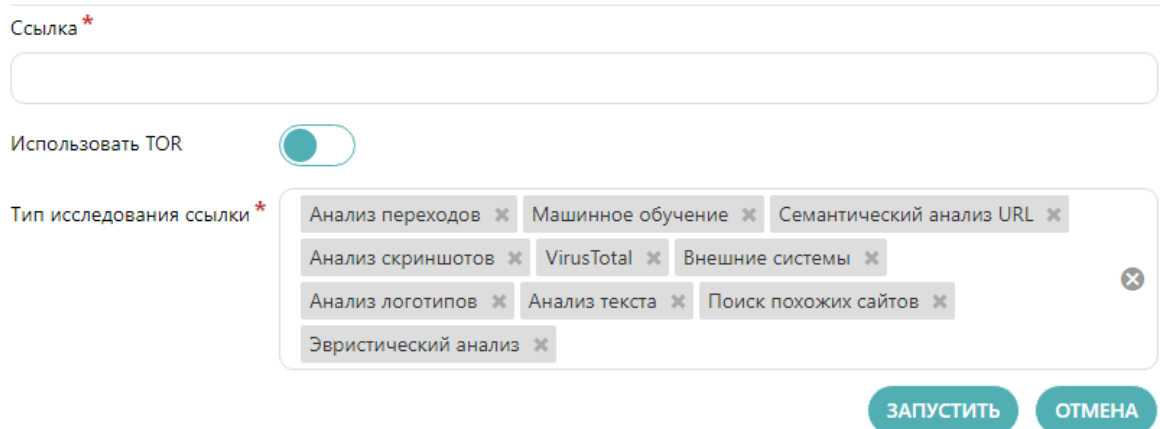


Рисунок 10. Форма создания исследования ссылки

8.2 Отчет по ссылке

В общей таблице ссылок отображаются все ссылки, прошедшие проверку в системе KAIROS. В таблице присутствует цветовая индикация вердикта ссылок: безопасный вердикт – зеленый цвет, подозрительный вердикт – желтый цвет, вредоносный вердикт – красный цвет (Рисунок 11).

Создано	Описание источника	Ссылка	Статус	Вердикт
10.06.2022, 08:40	sarkhangelsky@avs.w.ru	https://ru.wikipedia.org/wiki/%D0%A1%D0%BD%D0%88%D1%81%D0%BE%D0%BA_%D1%81%D0%80%D0%BC%D1%8B%D1%85_%D0%84%D0%B...	Завершено	Безопасный
10.06.2022, 08:40	sarkhangelsky@avs.w.ru	https://www.tmttr.ru/hobet/	Завершено	Безопасный
10.06.2022, 08:39	sarkhangelsky@avs.w.ru	https://el.wikipedia.org/wiki/%CE%99%CF%83%CE%BF%CF%81%CF%81%CE%BF%CF%80%CE%AF%CE%B1_%CF%87%CF%81%CF%8E%CE%BC%CE...	Завершено	Безопасный
10.06.2022, 08:39	sarkhangelsky@avs.w.ru	http://www.turboservisas.it	Завершено	Подозрительный
10.06.2022, 08:37	sarkhangelsky@avs.w.ru	https://bn.wikipedia.org/wiki/%E0%A6%B6%E0%A6%BE%E0%A6%9F%E0%A6%BE%E0%A6%B0_%E0%A6%B8%E0%A7%8D%E0%A6%AA%E0%A6%B...	Завершено	Безопасный
10.06.2022, 08:37	sarkhangelsky@avs.w.ru	https://ru.wikipedia.org/wiki/%D0%90%D0%B4%D0%B0%D0%BF%D1%82%D0%B5%D1%80_%D0%BE%D0%B1%D1%8A%D0%B5%D0%B4%D1%82...	Завершено	Безопасный
10.06.2022, 08:37	sarkhangelsky@avs.w.ru	https://www.atkomplekt.ru/hobet	Завершено	Безопасный
10.06.2022, 08:37	sarkhangelsky@avs.w.ru	https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%B7%D0%B5%D1%80%D0%8A%D0%B0%D0%8E%D1%8C%D0%BD%D1%8B%D0%B9...	Завершено	Безопасный
10.06.2022, 08:30	Bot_alive_phish	http://webmail.serveradmin.rpLco/	Завершено	Вредоносный
10.06.2022, 08:30	Bot_alive_phish	https://s.id/78qnl	Завершено	Вредоносный

Рисунок 11. Таблица ссылок

По каждой ссылке можно просмотреть отчет, обосновывающий присвоенный ей вердикт, нажав на иконку «Отчет» (Рисунок 12).

Отчет по ссылке

<http://www.turboservisas.it>

№ 308049 10.06.2022, 08:39:20 **ПОДОЗРИТЕЛЬНЫЙ**

SHA256 462764d932c5f8eef6bf8293fe010e9a0cae9ebf2253fee44456aad9f1e16ecf

Статус Завершено

Исследования

ID	Регистрация в системе ↓	Статус	Вердикт	Код ответа
430462	10.06.2022, 08:39	Завершено	Подозрительный	200

Рисунок 12. Отчет по ссылке

Для более детального ознакомления с результатами исследования ссылки необходимо перейти в отчет по исследованию, нажав на иконку «Отчет» вкладки «Исследования» в отчете по ссылке (Рисунок 15).

Также система предоставляет возможность изменения вердикта ссылки в ручном режиме. Для этого необходимо нажать на иконку «Изменить вердикт» напротив нужной ссылки и заполнить все требуемые поля в открывшейся форме (Рисунок 13).

ИЗМЕНЕНИЕ ВЕРДИКТА
✕

Вердикт * ▼
Подозрительный

Причина изменения вердикта * ▼

Новый вердикт будет иметь наивысший приоритет и не может быть изменен системой

СОХРАНИТЬ
ОТМЕНА

Рисунок 13. Форма изменения вердикта

9 Раздел «Исследования»

В таблице исследований можно отслеживать статус исследования веб-ссылок (Рисунок 14).

KAİROS
ИССЛЕДОВАНИЯ

СОЗДАТЬ

Страница 11889 из 11908 (Всего элементов: 119079) < 1 ... 11887 11888 11889 11890 ... 11908 >

⚙️ Перетащите столбец сюда, чтобы сгруппировать по нему

10 20 50 100
ЭКСПОРТ
15 сек.

☐	ID	Дата	Источник	Ссылка	Статус	Код	Вердикт	
<input type="checkbox"/>	313790	01.03.2022, 16:11	Telegram Bot	ffff.ru	Завершено	200	Вредоносный	📄 📄
<input type="checkbox"/>	313789	01.03.2022, 16:10	Telegram Bot	test.ru	Завершено	0	Безопасный	📄 📄
<input type="checkbox"/>	313788	01.03.2022, 15:04	Telegram Bot	fgHfghf.ru	Завершено	0	Подозрительный	📄 📄
<input type="checkbox"/>	313787	01.03.2022, 15:04	Telegram Bot	https://daily.afisha.ru/cities/22505-kak-spravitsya-s-trevogoy-iz-novostey-prostye-tehniki-ekstrennoy-samopomoshchi	Завершено	200	Безопасный	📄 📄
<input type="checkbox"/>	313786	28.02.2022, 17:46	KAİROS Flask_API	https://itgood.ru/2019/06/13/kak-proverit-versiju-paketa-linux-pered-ego-ustanovkoj/	Завершено	200	Безопасный	📄 📄
<input type="checkbox"/>	313785	28.02.2022, 17:16	Telegram Bot	https://gitlab.avsw.ru/machinelearning/linkchecker_bot_tg/-/releases/new	Завершено	0	Безопасный	📄 📄
<input type="checkbox"/>	313784	27.02.2022, 20:45	Telegram Bot	soldiers-mothers-rus.ru	Завершено	0	Подозрительный	📄 📄
<input type="checkbox"/>	313783	27.02.2022, 20:45	Telegram Bot	фонд-помощи-беженцам.рф	Завершено	200	Безопасный	📄 📄
<input type="checkbox"/>	313782	27.02.2022, 20:45	Telegram Bot	z-army.ru	Завершено	0	Безопасный	📄 📄
<input type="checkbox"/>	313781	27.02.2022, 20:45	Telegram Bot	zarmy.ru	Завершено	0	Безопасный	📄 📄

Страница 11889 из 11908 (Всего элементов: 119079) < 1 ... 11887 11888 11889 11890 ... 11908 >

Рисунок 14. Раздел «Исследования»

По каждому проведенному исследованию также можно просмотреть отчет, нажав на иконку «Отчет» напротив нужного исследования (Рисунок 15).

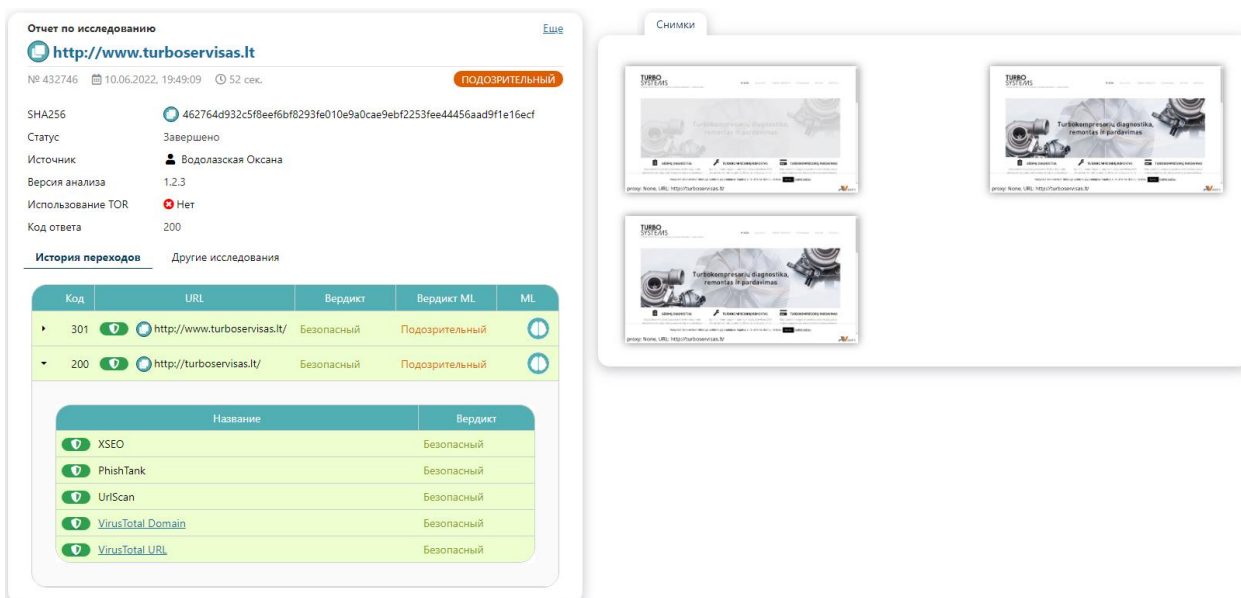


Рисунок 15. Отчет по исследованию

Отчет по исследованию веб-ссылки включает в себя параметры, описанные в таблице 6.

Таблица 6. Параметры отчета по исследованию

№	Параметр	Описание
1.	Общая информация	Значимые идентификационные параметры ссылки: <ul style="list-style-type: none"> – имя; – номер исследования; – дата и время запуска исследования; – длительность.
2.	SHA256	Контрольная сумма ссылки, которая может использоваться в качестве ее уникального идентификатора.
3.	Вердикт	Общий вердикт по ссылке в системе на основании всех источников анализа.
4.	Статус	Статус исследования ссылки в системе.
5.	Источник	Источник поступления ссылки на проверку в систему.
6.	Версия анализа	Версия модуля анализа ссылок, используемого для анализа в системе.

№	Параметр	Описание
7.	Использование TOR	Индикатор применения анонимизации трафика при переходе по ссылке.
8.	Код ответа	Ответ сервера при запросах по протоколу HTTPS.
9.	История переходов	Пути переходов веб-ссылки на другие адреса.
10.	Другие исследования	История исследований ссылки в системе.
11.	Машинное обучение	Модели машинного обучения, которые анализируют синтаксическую структуру файла на предмет наличия в ней вредоносных элементов.
12.	Снимки	Снимки экрана при отображении веб-страницы.

Машинное обучение включает в себя несколько моделей с разными типами алгоритмов (Рисунок 16).

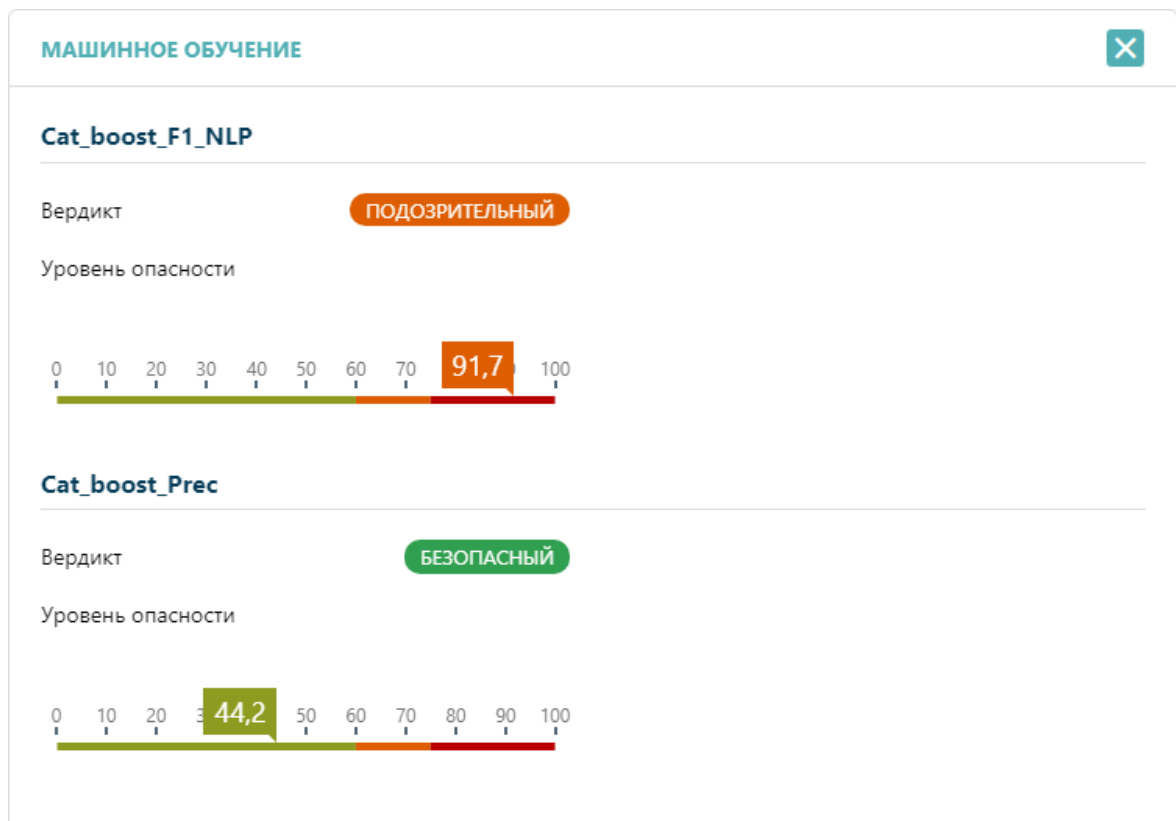


Рисунок 16. Модели машинного обучения

У каждой модели есть свой вердикт по объекту анализа и шкала с обозначением уровня опасности в процентном отношении.

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

- внешние аналитические ресурсы (XSEO, PhishTank, UrlScan)
- VirusTotal Domain
- VirusTotal URL
- модели машинного обучения

10 Раздел «Настройки»

В разделе «Настройки» осуществляется настройка всех модулей системы. Также в данном разделе реализована возможность импорта и экспорта настроек системы из файла и в файл соответственно (Рисунок 17).

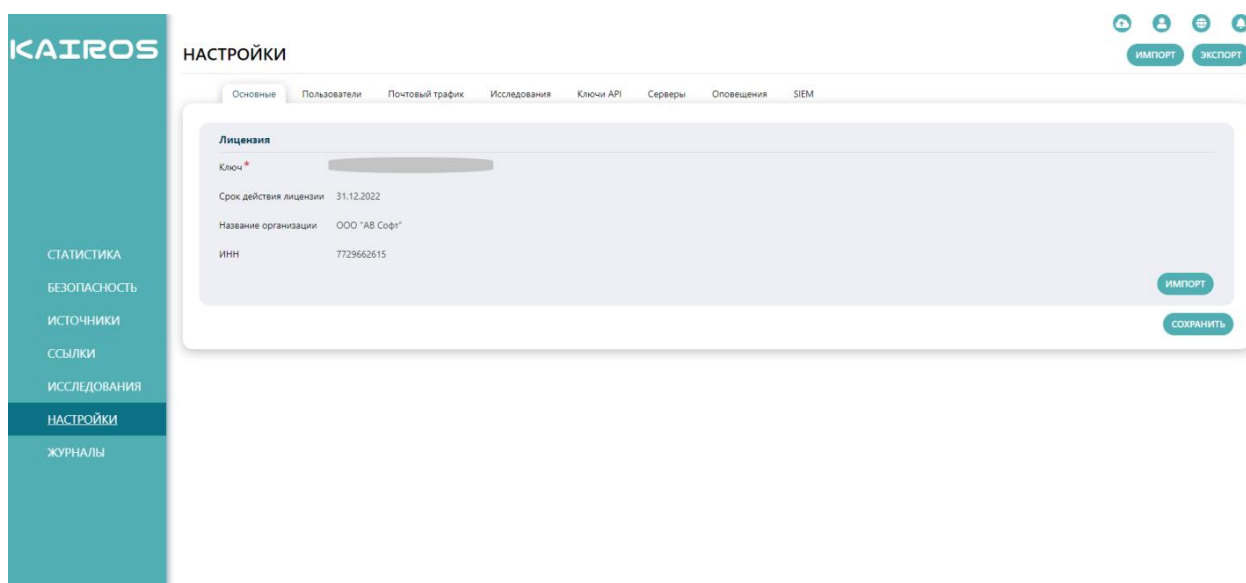


Рисунок 17. Раздел «Настройки», вкладка «Основные»

11 Раздел «Журналы»

В разделе «Журналы» присутствуют данные мониторинга значимых действий, процессов и ресурсов системы (Рисунок 18).

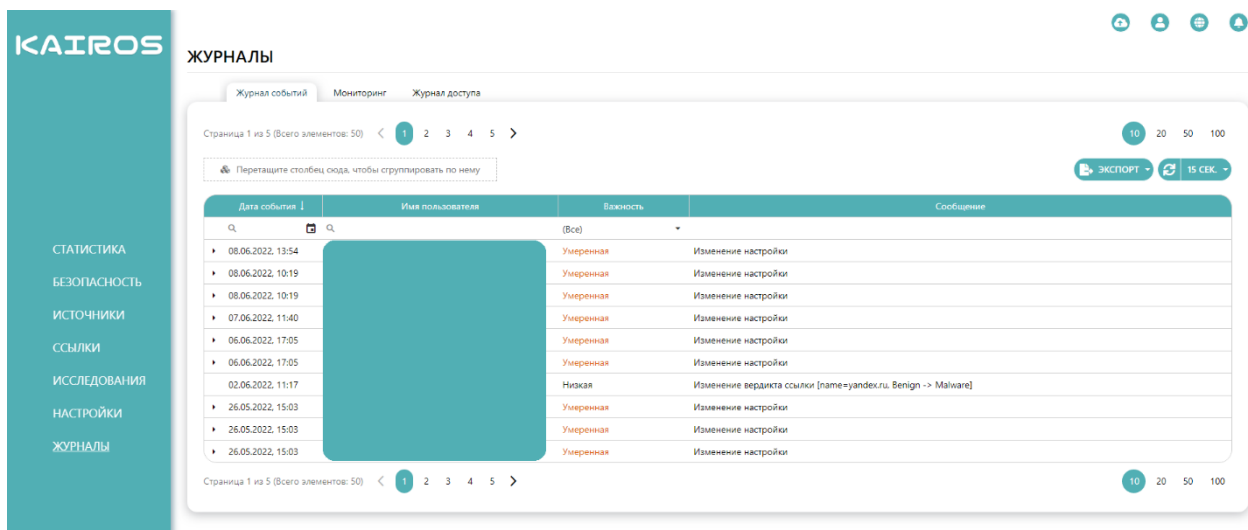


Рисунок 18. Раздел «Журналы», вкладка «Журнал событий»

Назначение вкладок в разделе «Журналы» описано в таблице 7.

7. 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.