



AVSOFT KAIROS

Система защиты от спама и фишинга

Функциональные характеристики

**Москва
2022**

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

Апрель 08, 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	Общие положения	4
2	Базовые функциональные возможности.....	4
3	Расширенные функциональные возможности	7

1 Общие положения

В настоящем документе описаны функциональные возможности системы защиты от спама и фишинга AVSOFT KAIROS (далее - Система KAIROS).

Система KAIROS работает на основе технологий почтового шлюза и систем защиты от спама и фишинга. Ее основная задача — проверка объектов анализа на спам, фишинг, вредоносное программное обеспечение.

Проверка в системе KAIROS включает в себя несколько параллельных исследований множеством инструментов, каждый из которых имеет свой вердикт, окончательное решение принимается по высшему вердикту. По окончании исследования выдается подробный отчет.

2 Базовые функциональные возможности

Система KAIROS принимает на проверку данные из различных источников:

- веб-трафик
- почтовый трафик
- мессенджеры
- ручная загрузка
- API интерфейс

Система KAIROS способна анализировать следующие типы данных:

- Атрибуты электронных писем
- Текстовое содержание электронных писем
- Веб-ссылки
- QR коды
- Файлы

Система KAIROS обеспечивает защиту от следующих видов угроз информационной безопасности:

- Спам
- Фишинг
- Вредоносное программное обеспечение

Система KAIROS имеет возможность проверять следующие записи сетевого домена:

- DKIM
- DMARK
- SPF

Система KAIROS имеет модели машинного обучения, которые по основным и косвенным признакам выносят самостоятельный вердикт относительно текстового контента электронного письма на предмет его отношения к спаму.

Система KAIROS способна проводить анализ заголовков электронных писем по следующим параметрам:

- Received
- Reply-To
- Received-SPF
- DKIM
- X-Headers
- X-Distribution
- To
- Bcc
- Date
- Message-ID
- X-UIDL

Проверка веб-ссылок на фишинг осуществляется одновременно в следующих направлениях:

- Внешние аналитические источники
- Модели машинного обучения
- Проверка переходов
- Статический анализ

Виды моделей машинного обучения для анализа веб-ссылок на фишинг:

- RandomForest (PHISHING.dill)
- Нейронная сеть (neuro_PHISHING.h5)
- Catboost (model_Cat_*)

Система KAIROS позволяет проверять следующие типы файлов:

- Исполняемые файлы (EXE, ELF, CMD)
- Офисные документы (DOCX, DOTM, XLSX, PPTX, PDF, RTF)
- Мобильные приложения (APK)

- Архивы, включая многотомные и защищенные паролем (ZIP, JAR, RAR, 7Z)
- Скрипты (BAT, SH) и др.
- Почтовые форматы, в том числе EML и MSG.

Проверка файлов осуществляется следующими методами анализа:

- Контрольная сумма
- Антивирусный движок

Система KAIROS обеспечивает распаковку и расшифровку по словарю следующих типов файлов:

- Архивов
- Файлов
- PDF

Система KAIROS позволяет осуществлять настройку следующих типов политик:

- Фильтрация по типам файлов
- Репутация отправителя
- Рейтинг получателя
- SMTP сессии
- Домены
- Спам

Система KAIROS имеет систему очередей с возможностью повышения приоритета проверки для привилегированной категории и настройки правил проверки для разных групп пользователей.

Система KAIROS поддерживает интеграцию со следующими типами систем:

- Межсетевой экран
- Почтовый шлюз
- Active Directory
- Мультисканер
- SIEM/SOAR
- Песочница

Система KAIROS поддерживает интеграцию с внешними системами по следующим протоколам:

- SMTP
- POP3/POP3S
- IMAP/IMAPS
- ICAP
- REST API
- SYSLOG

Система KAIROS поддерживает следующие варианты установки:

- Физический сервер
- Виртуальная среда
- Облачная среда

Почтовый трафик может проверяться в разных режимах:

- Зеркало
- В перерыве
- Архивная папка
- Протокол REST API

3 Расширенные функциональные возможности

Машинное обучение позволяет автоматически обнаруживать спам и фишинг на основе ретроспективного анализа баз данных, накопленных в системе KAIROS. Изучив большое количество образцов, модель машинного обучения способна обобщать информацию и обнаруживать новые виды спама и фишинга.

В системе KAIROS для классификации и обработки текстов используются модели на базе новой технологии – трансформеры. Они хорошо понимают контекст предложения, его настроение и общий смысл, что позволяет эффективно идентифицировать спам.

Для получения вектора признаков используется концепция вложений (embeddings), которая способна определять связи между словами, их многозначность, последовательность, преобразование, контекст, частоту употребления.

Система KAIROS позволяет в автоматическом режиме дообучать модули машинного обучения в том числе на данных пользователя.