

ОБЩАЯ ИНФОРМАЦИЯ

Система AVSOFT KAIROS — мультимодульный аналитический инструмент на базе почтового шлюза для управления потоками электронной почты с учетом корпоративных стандартов и политик безопасности. Система сканирует и анализирует всю входящую и исходящую электронную почту на предмет спама, фишинга и вредоносных вложений.

Проверка в 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.

Система KAIROS принимает на проверку данные из различных источников:



Почтовый трафик



Ручная загрузка



API интерфейс



ICAP

Система KAIROS способна анализировать следующие типы данных:

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

УГРОЗЫ

Система KAIROS обеспечивает защиту от следующих видов угроз информационной безопасности:



Спам и массовые рекламные рассылки



Массовый и целевой фишинг



DDoS-атаки на почтовые серверы



Вредоносное программное обеспечение



BEC-атаки (Business Email Compromise)



Социальная инженерия



Уведомления о статусе доставки (DSN)



Атаки сбора каталогов (DHA, d harvest attacks)

АНТИСПАМ

Система KAIROS выполняет многоступенчатую проверку электронных писем, включающую:

- Анализ SMTP-сессии
- Первичная проверка
- Глубокий анализ вложений — ссылок и файлов
- Анализ заголовков и текстового содержимого

Используемые технологии:

- Проверка подлинности отправителя по стандартам SPF, DKIM, DMARC
- Автоматическая классификация текста с помощью моделей машинного обучения, выявляющих спам и тематические категории
- Применение серых и чёрных списков отправителей
- Анализ заголовков с использованием индикаторов
- Фильтрация по ключевым словам

ФИШИНГ

Проверка веб-ссылок на фишинг в системе KAIROS осуществляется по следующим направлениям:

Статический анализ:

- Использование внешних аналитических сервисов: VirusTotal, XSEO, UrlScan, GoogleReport, MetaDefender, NordVPN, NortonSafeweb, SURBL
- Проверка ссылок по внутренним базам данных, включая регулярные выражения, списки безопасных и вредоносных доменов
- Применение моделей машинного обучения для выявления подозрительных признаков

Динамический анализ:



Анализ мгновенных редиректов и выявление отложенных перенаправлений



Выгрузка и отправка на анализ файлов по ссылкам из облачных хранилищ и прямых URL



Сбор и проверка информации по домену и HTTP-заголовкам



Исследование артефактов и содержимого сайта



Визуальный анализ страниц сайтов



Извлечение и проверка ссылок из QR-кодов на скриншотах сайтов

Дополнительные возможности

Поддержка проверки “спящих ссылок” — ссылки проверяются динамически в момент их активации пользователем, обеспечивая актуальную защиту от скрытых угроз

Анализ ссылок, извлеченных из QR-кодов, содержащихся в теле письма или в файловых вложениях, а также на страницах веб-сайтов

Модели машинного обучения используются для:

- Обнаружение доменов с генерацией алгоритмическими методами (DGA)
- Определение признаков киберсквоттинга и тайпсквоттинга (опечаток и подмен доменного имени)
- Оценка визуального сходства сайтов для выявления подмен и фишинга
- Проведение эвристического анализа и детальный анализ содержимого страницы для выявления широкого спектра угроз

ФАЙЛЫ

Система KAIROS позволяет проверять следующие типы файлов:

-  Офисные документы (DOCX, DOTM, XLSX, PPTX, PDF, RTF и др.)
-  Исполняемые файлы (EXE, ELF, CMD и др.)
-  Мобильные приложения (APK)
-  Скрипты (BAT, SH и др.)
-  Архивы, включая многотомные и защищенные паролем (ZIP, JAR, RAR, 7Z и др.)
-  Почтовые форматы, в том числе EML и MSG

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



Архивов



Файлов



PDF

ПОЛИТИКИ

Система KAIROS позволяет создавать и настраивать политики безопасности и фильтрации сообщений по следующим критериям:

-  Фильтрация по расширениям и mime-типам файлов
-  Тематика письма
-  Репутация отправителя
-  SMTP сессии
-  Рейтинг получателя
-  Спам

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

ИНТЕГРАЦИИ

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
- ICAP
- REST API
- SYSLOG

ИНСТАЛЛЯЦИЯ И РЕЖИМЫ ПРОВЕРКИ

Система KAIROS поддерживает следующие варианты установки:



Физический
сервер



Виртуальная
среда



Облачная
среда

Версии ОС для развертывания системы:

Astra Linux

Ubuntu

Debian

Почтовый трафик может проверяться в разных режимах:

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

МАШИННОЕ ОБУЧЕНИЕ

Система KAIROS использует технологии машинного обучения и глубоких нейронных сетей на базе трансформеров для эффективного обнаружения спама и фишинга.

Объекты, анализируемые при помощи моделей машинного обучения:

-  Текстовое содержимое и заголовки письма
-  Веб-ссылки (URL и HTML-страницы)
-  QR-коды
-  Визуальный анализ скриншотов (извлечение QR-кодов, обнаружение клонов)

Благодаря комплексному семантическому анализу, включая понимание контекста и общего смысла предложения, модели выявляют новые виды спама и фишинга.

Для представления и обработки данных используется концепция векторного представления (embeddings), которая позволяет учитывать связи между словами, их многозначность, последовательность, а также частотные зависимости.

Использование мультязычных моделей расширяет охват системы. Система KAIROS позволяет в автоматическом режиме дообучать модели машинного обучения в том числе на данных пользователя