

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «F6 Digital Risk Protection»

Описание функциональных характеристик

Содержание

| | |
|-----------------------------------------------------------|----------|
| ТЕРМИНЫ И СОКРАЩЕНИЯ | 3 |
| 1 ОБЩИЕ СВЕДЕНИЯ | 4 |
| 1.1 Введение..... | 4 |
| 1.2 Назначение ПО..... | 4 |
| 1.3 Программно-аппаратные среды функционирования ПО | 4 |
| 2 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО | 5 |
| 3 РЕАЛИЗАЦИЯ ПО | 7 |
| 3.1 Функциональные возможности ПО | 7 |
| 3.2 Состав ПО | 7 |
| 3.3 Функции частей ПО | 8 |
| 3.3.1 Модуль мониторинга сети Интернет | 8 |
| 3.3.2 Модуль анализа объекта в системе | 8 |
| 3.3.3 Модуль реагирования | 8 |

ТЕРМИНЫ И СОКРАЩЕНИЯ

| Термин | Описание |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Заказчик | Лицо, которое использует на законных основаниях ПО на основании заключенного договора |
| Исполнитель | Работы Исполнителя на протяжении всего жизненного цикла могут выполняться: <ul style="list-style-type: none">• АО «БУДУЩЕЕ»;• Компанией-интегратором, по выбору Заказчика |
| ПО | Программное обеспечение «F6 Digital Risk Protection» |
| Разработчик | АО «БУДУЩЕЕ» |
| Скоринг | Система оценки объекта |
| Скриншот | Изображение, «снимок» экрана ПК или мобильного устройства, на котором запечатлено содержимое экрана устройства |

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание функциональных характеристик программного обеспечения «F6 Digital Risk Protection» (далее — ПО, Digital Risk Protection, Система).

1.2 Назначение ПО

«F6 Digital Risk Protection» – платформа по защите цифрового присутствия компании в сети Интернет, мониторингу и противодействию цифровым рискам. Платформа собирает данные из различных источников с помощью автоматических средств мониторинга на предмет незаконного использования бренда или объектов интеллектуальной собственности компании. Для реагирования на такие нарушения платформа использует систему автоматизированного реагирования для исполнения требований устранить нарушение.

1.3 Программно-аппаратные среды функционирования ПО

ПО «F6 Digital Risk Protection» не требует установки на устройстве Пользователя.

ПО поставляется Заказчику двумя способами:

1. ПО как услуга (SaaS) – облачный интернет-сервис;
2. Доступ через API-интерфейс.

Требования для работы ПО как облачного интернет-сервиса:

- Windows Internet Explorer версии 11.0 и выше;
- Google Chrome версии 8.6.395 и выше;
- Mozilla Firefox версии 82.0.1 и выше;
- Apple Safari версии 14.0 и выше;
- Opera версии 10.5 и выше;
- iOS Safari версии 14.0 и выше;
- Opera Mobile версии 10.0 и выше;
- Google Chrome for Android версии 11.0 и выше;
- Mozilla Firefox for Android версии 82.0 и выше;
- Windows Internet Explorer Mobile версии 10.0 и выше;
- Яндекс.Браузер версии 20 и выше;
- Microsoft Edge версии 105 и выше.

Требования для работы ПО с помощью API-интерфейса:

- Python 3.5.3.

2 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

ПО «F6 Digital Risk Protection» собирает данные из различных источников в сети Интернет с помощью автоматических средств мониторинга. Мониторинг цифровых активов компании производится в таких ресурсах, как:

- Веб-страницы;
- Базы доменных имен;
- Базы фишинговых и мошеннических ресурсов;
- Поисковые системы и контекстная реклама;
- Социальные сети и мессенджеры;
- Площадки для размещения мобильных приложений;
- Торговые площадки и платформы объявлений;
- Публичные массовые базы данных и открытые репозитории кода;
- DarkWeb-форумы («теневые», подпольные форумы злоумышленников).

Данные из публичных баз данных, открытых репозиториях кода и darkweb-форумов ПО получает через интеграцию с ПО «**F6 Threat Intelligence**».

Полученные данные представлены в виде ссылок, которые ПО анализирует на предмет нелегального использования бренда и интеллектуальной собственности компании. Собранные данные могут содержать скриншоты, изображения, HTML-файлы, источники трафика и связанные с доменом параметры. Результатом анализа являются следующие параметры, доступные в теле объекта (ссылки):

- Статус и тип нарушения;
- Последний снятый при проверке ресурса скриншот;
- Общий скоринг опасности объекта;
- Скоринг обнаружения логотипа вашего бренда;
- Скоринг доменного имени;
- Информация о регистраторе доменного имени;
- Информация о хостинг-провайдере ресурса и администраторе ресурса.

После приобретения ссылкой статуса и типа нарушения, нелегитимное использование бренда подтверждается клиентом в интерфейсе ПО. Далее запускается процесс реагирования, целью которого является пресечение нелегитимной активности и итоговое устранение нарушений.

Для реагирования на такие нарушения платформа использует систему автоматизированного реагирования для исполнения требований устранить нарушение.

Первым этапом владельца ресурса с нарушением оповещают о наличии такого нарушения и запрашивают устранить его. Вторым этапом оповещают хостинг-провайдера и регистратора ресурса для устранения нарушения. Нарушения по возможности устраняются. В случае, если нарушение не было устранено, происходит эскалация – применение дополнительных мер по устранению нарушения:

- Запрос на добавление ресурса в базы мошеннических и фишинговых ресурсов;
- Запрос на удаление ресурса из поисковой выдачи и блокировка контекстной рекламы;
- Запрос на блокировку мошеннических аккаунтов в социальных сетях;
- Запрос на блокировку ресурса на уровне DNS-серверов.

Большинство нарушений (85%) устраняются в досудебном порядке.

«F6 Digital Risk Protection» также позволяет использовать графовый анализ, который помогает выявить инфраструктуру киберпреступников и найти дополнительные методы для успешного устранения нарушений.

3 РЕАЛИЗАЦИЯ ПО

3.1 Функциональные возможности ПО

ПО обладает следующими функциональными возможностями:

- Сбор текстовых и графических данных из следующих источников: социальные сети, регулярные веб-сайты, магазины (площадки для размещения) мобильных приложений, контекстная реклама, мессенджеры (мессенджер Телеграм), доски объявлений;
- Категоризация данных при помощи регулярных выражений (текстовые данные) и нейронных сетей (графические данные);
- Формирование пакета данных для использования в последующем устранении выявленного риска: скриншот страницы, html-файл, данные о времени и программно-аппаратной среде проверки страницы сайта в сети Интернет, контактные данные регистратора доменного имени/провайдера услуг хостинга;
- Отображение статистической информации о ходе сбора/анализа данных на единой контрольной панели.

3.2 Состав ПО

ПО «F6 Digital Risk Protection» представляет из себя комплексную систему, состоящую из нескольких модулей. ПО реализовано на следующих языках программирования:

- JavaScript
- Typescript (версия 5.1)
- PHP (версия 7.2)
- Python (версия 3.9)
- Golang (версия 1.21)

ПО состоит из следующих модулей:

- Модуль мониторинга сети Интернет;
- Модуль анализа объекта в системе (ссылки);
- Модуль реагирования.

В рамках предоставляемого интерфейса операторы ПО имеют возможность выгружать базовую отчетность об актуальном состоянии объектов (ссылок).

3.3 Функции частей ПО

3.3.1 Модуль мониторинга сети Интернет

Модуль собирает данные из различных источников в сети Интернет с помощью автоматических средств мониторинга. Мониторинг цифровых активов компании производится по следующим источникам данных:

- Веб – поисковая выдача и доменные имена;
- Социальные сети;
- Доски объявлений;
- Реклама – рекламные объявления;
- Мобильные приложения;
- Мессенджеры.

Доступ к модулю предоставляется через веб-интерфейс. Полученные из источников данные представлены в виде ссылок. Каждая ссылка содержит информацию о статусе нарушения, типе нарушения и бренде, к которому относится нарушение.

3.3.2 Модуль анализа объекта в системе

Модуль анализирует полученные *Модулем мониторинга сети Интернет* данные на предмет нелегального использования бренда или интеллектуальной собственности компании. Модуль распознает и анализирует логотипы бренда, доменные имена, а также анализирует HTML-код веб-страниц. В результате анализа каждой ссылке присваиваются:

- Статус и тип нарушения;
- Последний снятый при проверке ресурса скриншот;
- Общий скоринг опасности объекта;
- Скоринг обнаружения логотипа вашего бренда;
- Скоринг доменного имени;
- Информация о регистраторе доменного имени;
- Информация о хостинг-провайдере ресурса и администраторе ресурса.

Обработанные данные отображаются в разделе «Нарушения» веб-интерфейса ПО. Модуль поддерживает стандартный формат импорта данных CSV.

3.3.3 Модуль реагирования

Модуль позволяет операторам Системы (сотрудники Разработчика) реагировать на нарушения, обнаруженные в процессе мониторинга и анализа данных в сети Интернет. В результате реагирования создается жалоба к регулятору с запросом устранить нарушение.

Доступ к модулю предоставляется через веб-интерфейс. В рамках интерфейса модуль обеспечивает операторам Системы следующие функции:

- Доступ к контактным данным регулятора (хостинг-провайдера, регистратора или других регулирующих органов);
- Функционал по автоматическому сбору жалоб на ресурсы в зависимости от нарушения, регулятора или настроенных операторами частных правил;
- Почтовый клиент для общения с регуляторами в рамках одного нарушения;
- Создание и редактирование текстовых блоков, которые в дальнейшем используются для создания жалобы на то или иное нарушение.