

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «F.A.C.C.T. Digital Risk Protection»

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ	3
1.1 Введение	3
2 КРАТКОЕ ОПИСАНИЕ И НАЗНАЧЕНИЕ ПО	3
3 ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПО.....	3
4 ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ К ПО	4
5 ПРОГРАММНО-АППАРАТНЫЕ СРЕДЫ ФУНКЦИОНИРОВАНИЯ ПО	4
6 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО	5
7 РЕАЛИЗАЦИЯ ПО	5
7.1 Модуль мониторинга сети Интернет	5
7.2 Модуль анализа объекта в системе.....	6
8 УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ ПО	6

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

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

2 КРАТКОЕ ОПИСАНИЕ И НАЗНАЧЕНИЕ ПО

Digital Risk Protection – Программное обеспечение для обнаружения, анализа и устранения нелегитимной активности, связанной с цифровыми активами компании. В продукте используются машинное обучение и нейронные сети для анализа больших данных, экспертные скоринговые модели, анализ трафика, графовый анализ связанных ресурсов, а также выделенные каналы связи и методы взаимодействия с регуляторами сети Интернет, выработанные годами.

Основными целями создания Системы являются:

- Предоставление интерфейса с отображением результатов мониторинга сети Интернет;
- Создание возможности взаимодействия в режиме реального времени;
- Повышение качества и количества обнаруживаемых нарушений;
- Предоставление прозрачной статистической и аналитической информации.

3 ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ПО

ПО обладает следующими 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 в ходе категоризации 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.

4 ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ К ПО

В ходе эксплуатации ПО должны выполняться следующие требования:

- Совместимость – ПО должно быть совместимо с наиболее популярными программно-аппаратными средами (указаны в п.5 «Программно-аппаратные среды функционирования ПО»);
- Универсальность – возможность использования поисковых и ключевых слов и выражений для осуществления настроек поиска на различных типах площадок сети Интернет;
- Обеспечение точности полученных результатов – осуществление многоэтапных проверок наличия текстовых/графических данных на страницах площадок сети Интернет;
- Надежность – обеспечение бесперебойной работоспособности ПО не ниже 90% времени на протяжении года.

5 ПРОГРАММНО-АППАРАТНЫЕ СРЕДЫ ФУНКЦИОНИРОВАНИЯ ПО

ПО функционирует в следующих программно-аппаратных средах:

- 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

6 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

Внутри Системы используется набор виртуальных машин с различными операционными системами. Система производит поиск по ключевым словам и регулярным выражениям в сети Интернет на наличие объектов (ссылок), содержащих в себе потенциальные нарушения. Анализируемая ссылка в автоматизированном режиме запускается на виртуальной машине для снятия «мгновенного снимка» и проходит множество проверок перед обновлением информации в пользовательском интерфейсе. В результате анализа каждый объект (ссылка) получает статус и тип потенциального нарушения. В интерфейсе доступна следующая информация об объекте:

- Дата обнаружения ссылки;
- Тип нарушения;
- Скриншот, снятый при проверке потенциально опасного ресурса;
- Скоринг объекта;
- Скоринг обнаружения логотипа вашего бренда;
- Скоринг доменного имени;
- Блок с информацией о регистраторе доменного имени;
- Блок с информацией о хостинг-провайдере ресурса;

После подтверждения нелегитимного использования интеллектуальной собственности Заказчика запускается процесс реагирования, целью которого является пресечение нелегитимной активности и итоговое устранение нарушений.

7 РЕАЛИЗАЦИЯ ПО

Система состоит из следующих модулей:

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

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

7.1 Модуль мониторинга сети Интернет

Модуль отвечает за сбор информации в сети Интернет по различным источникам данных:

- Веб – поисковая выдача и доменные имена;

- Социальные сети;
- Доски объявлений;
- Реклама – рекламные объявления;
- Мобильные приложения;
- Мессенджеры.

Модуль производит поиск ресурсов, которые содержат потенциальные нарушения. Доступ к модулю предоставляется через пользовательский 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.

7.2 Модуль анализа объекта в системе

Модуль производит автоматическую проверку полученных объектов и создает пакет данных для дальнейшей обработки нарушений. Обработанные объекты представлены в виде списка в пользовательском интерфейсе. При нажатии на отдельный элемент списка открывается окно с подробной информацией о потенциально опасном ресурсе. В окне отображается следующая информация:

- Текстовое превью, URL и название бренда;
- Дата обнаружения ссылки;
- Статус и тип нарушения;
- Последний снятый при проверке ресурса скриншот;
- Общий и детальный скоринг опасности объекта;
- Кнопки для скачивания скриншота и html файла;
- Блок с информацией о регистраторе доменного имени;
- Блок с информацией о хостинг-провайдере ресурса;
- Блок с информацией об администраторе ресурса.

8 УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ ПО

Устранение неисправностей ПО происходит в 2 этапа:

- Устранение критичных неисправностей. Производится непосредственно при обнаружении неисправности, выпуск исправляющего обновления производится незамедлительно.
- Устранение неисправностей не являющихся критическими. Производится в равно запланированные промежутки времени (раз в 2 недели) одновременно с выпуском других обновлений.