ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Digital Risk Protection»

Руководство по установке и эксплуатации ПО

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	**Описание**
Бренд	Совокупность уникальных идентификационных признаков, отличающих компанию. К составляющим бренда относят название, логотип, слоган, фирменный шрифт и т.п.
ВПО	Вредоносное программное обеспечение
Заказчик	Лицо, которое использует на законных основаниях ПО на основании заключенного договора
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО "Ф6 Инновации"; • Компанией-интегратором, по выбору Заказчика
ПО	Программное обеспечение «F6 Digital Risk Protection»
Разработчик	АО "Ф6 Инновации"
Сигнатура	Уникальный код, который ассоциируется с определенным документом, сообщением, программным обеспечением или любым другим объектом
Скриншот	Изображение, «снимок» экрана ПК или мобильного устройства, на котором запечатлено содержимое экрана устройства
Угроза	Потенциально - возможное происшествие, преднамеренное или нет, которое может оказать нежелательное воздействие на систему или хранящуюся информацию (т.е. нечто плохое, что может произойти)
Уязвимость	Недостаток в программном обеспечении, оборудовании или системе информационной

	безопасности, который позволяет киберпреступникам получить несанкционированный доступ к устройству либо ограничить доступ к сервису
Фишинг	Вид мошенничества, направленный на сбор конфиденциальной информации о пользователях, такой как логины, пароли, данные банковских карт и счетов, а также другой информации, которая может помочь злоумышленникам получить доступ к личным аккаунтам на сайтах, сервисам интернет-банкинга и т.д.
API	Application Programming Interface. Программный интерфейс, то есть описание способов взаимодействия одной компьютерной программы с другими
Darkweb (даркверб)	"Темная сеть", скрытая анонимная сеть интернета, где действуют злоумышленники, а также форумы в открытом Интернете, посвященные хакерской тематике
RESTful	REST (Representational State Transfer) — это способ создания API с помощью протокола HTTP. RESTful – это архитектурный стиль для операций по работе с сервером
SaaS	Software as a Service. Модель обслуживания, при которой программное обеспечение размещено в облачной инфраструктуре

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит руководство по установке и эксплуатации 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.

2 НАЧАЛО РАБОТЫ

«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.

2.1 Программно-аппаратные среды функционирования ПО

Требования для работы ПО как облачного интернет-сервиса:

- 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;
- Яндекс.Браузер версии 20 и выше;
- Microsoft Edge версии 105 и выше.

Требования для работы ПО с помощью API-интерфейса:

- Python 3.5.3.

2.2 Создание учетной записи

Для доступа к ПО необходима учетная запись пользователя системы. Перед началом работы с ПО необходимо обратиться к сотрудникам Разработчика и предоставить следующие данные:

- ФИО сотрудника;
- Адрес электронной почты сотрудника.

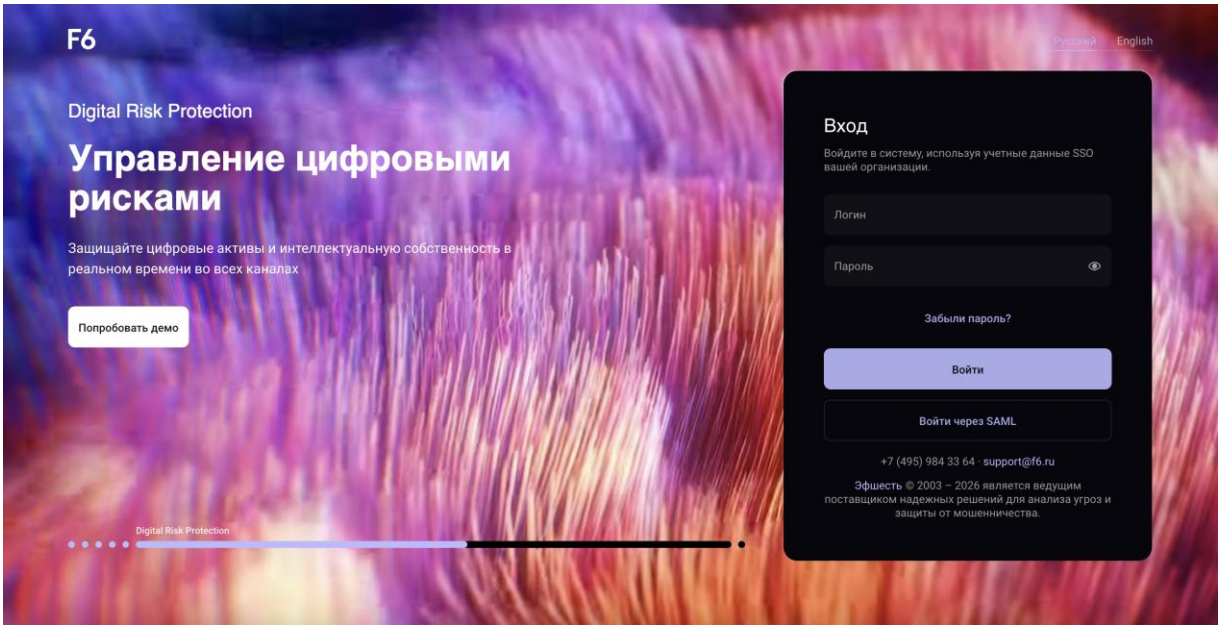
На указанную почту придет письмо для активации учетной записи. Необходимо перейти по ссылке и задать пароль для учетной записи. Пароль должен содержать:

- не менее 8 символов;
- прописные и строчные латинские буквы;
- числа;
- специальные символы.

2.3 Вход в учетную запись

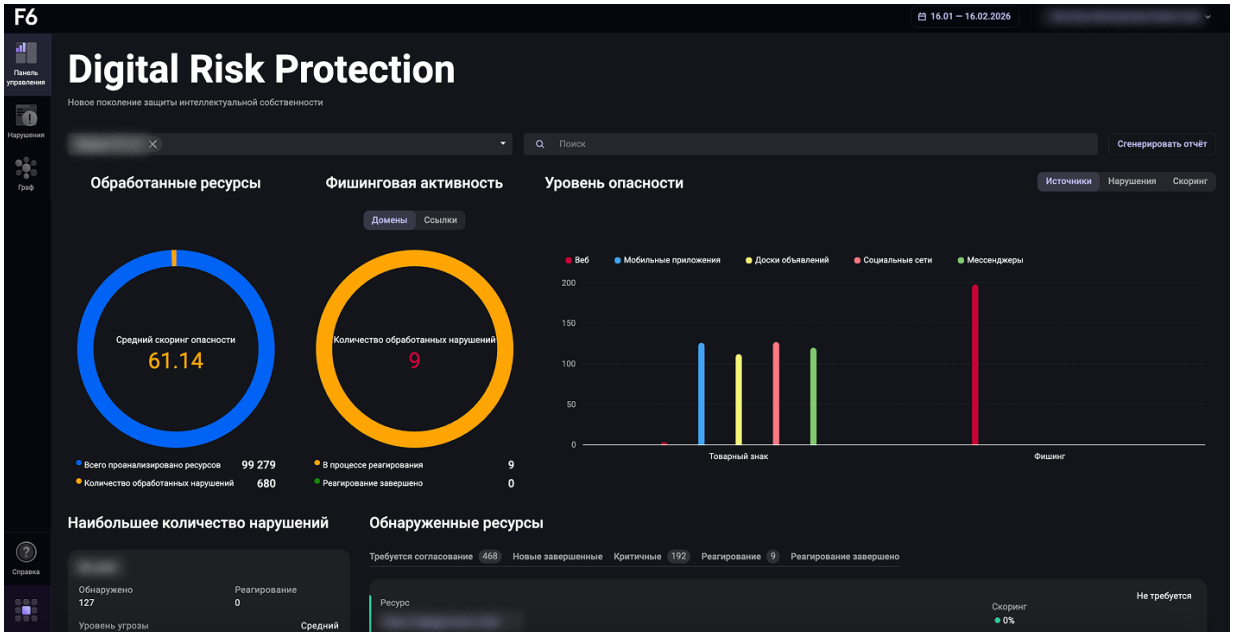
Для начала работы с ПО выполните следующие действия:

1. Откройте браузер и обратитесь к веб-интерфейсу ПО по адресу https://sso.f6.security/. Откроется страница авторизации:



2. Введите логин и пароль в соответствующие поля;

3. Нажмите кнопку «**Войти**». После успешной авторизации отобразится главная страница «F6 Digital Risk Protection».



После обновления системы при первом входе Пользователь увидит всплывающее окно с кратким обзором последних изменений.

При возникновении проблем со входом в платформу ПО обратитесь к сотрудникам Разработчика по электронной почте info@f6.ru.

2.4 Доступ к ПО с помощью API-интерфейса

API – программный интерфейс для получения данных и предназначенный для интеграции «F6 Digital Risk Protection» с системами внутренней безопасности и защиты от

мошеннических действий Заказчика. API использует протокол RESTful. Данные возвращаются в формате JSON.

Для доступа к API-интерфейсу ПО необходимо:

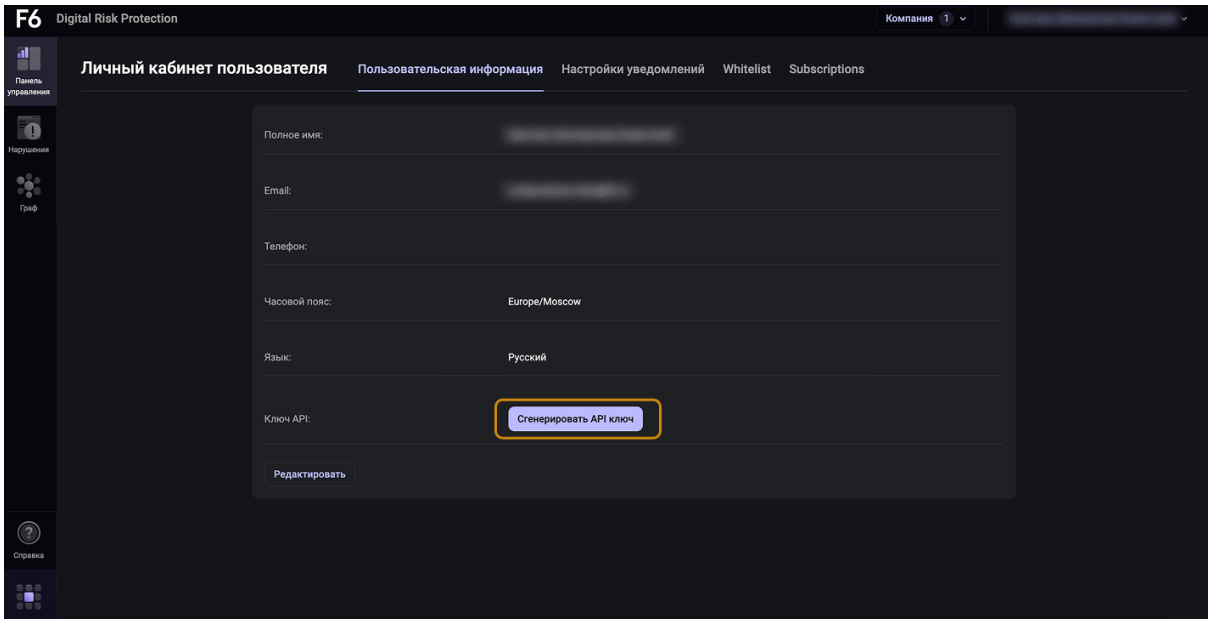
1. Предоставить ваши публичные IP-адреса, чтобы мы могли внести их в белый список для доступа к API;
2. Войти в свою учетную запись (см. **2.2 Создание учетной записи**), сгенерировать и сохранить API-ключ в вашем Профиле;
3. Внести следующие IP- и URL-адреса в список доступа своих систем внутренней безопасности:

IP-адреса	URL-адреса
• 46.148.232.110 • 212.41.15.111 • 84.38.186.218	• drp.f6.security (для доступа к веб-порталу и API) • sso.f6.security (требуется для доступа к интерфейсу)

2.4.1 Генерация API-ключа

Чтобы сгенерировать API-ключ перейдите в интерфейс системы Digital Risk Protection и выполните следующие шаги:

1. Перейдите на страницу https://drp.f6.security/;
2. Кликните на своё имя в правом верхнем углу и выберите «**Личный кабинет**»;
3. Нажмите кнопку «**Сгенерировать API ключ**»;

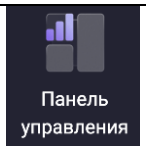
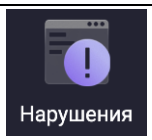
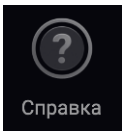


4. Нажмите на появившуюся строку с API-ключом и нажмите «**Скопировать**».

***Примечание**: Сохраните ключ в локальной директории или в хранилище ключей. Ключ НЕ сохранится в Личном кабинете.*

3 ИНТЕРФЕЙС ПО

Работа с ПО представляет собой взаимодействие с пользовательским интерфейсом ПО (далее – Система). Все разделы интерфейса доступны в боковой панели.

Раздел		Описание
	Панель управления	Главная страница ПО. Содержит виджеты с различными данными и статистикой
	Нарушения	Раздел содержит информацию о ресурсах, где было замечено незаконное использование бренда или объектов интеллектуальной собственности компании
	Справка	Раздел содержит документацию к ПО, соглашения и лицензии

Далее будут описана работа с ключевыми разделами ПО.

3.1 Панель управления

Раздел **Панель управления** содержит виджеты с различными данными и статистикой.

Виджет	Описание
Обработанные ресурсы	Общее количество обнаруженных ресурсов
Фишинговая активность	Общее количество обработанных фишинговых активностей, релевантных для компании Пользователя
Уровень опасности	Статистика частоты возникновения различных типов нарушений в разных источниках; средняя оценка риска
Наибольшее количество нарушений	Список доменных имен с максимальным количеством выявленных нарушений
Обнаруженные ресурсы	Виджет для быстрого доступа к информации из раздела **Нарушения**
Новости и отчеты	Информационный виджет, содержит последние новости по теме «Защита от цифровых рисков», исследования по работе по защите от цифровых рисков и отчеты
Уровень активности	Виджет отображает на временной шкале количество ресурсов с нарушениями, обнаруженными Системой
География нарушений	Карта мира с индикаторами. Эти индикаторы показывают географическое расположение хостинговых ресурсов, на

Виджет	Описание
	которых были обнаружены нарушения, релевантные для компании Пользователя

3.1.1 Действия с Панелью управления

В верхней части страницы расположены окно выбора компании, строка поиска и кнопка «**Сгенерировать отчет**».

С помощью окна выбора компании Пользователь может выбрать бренд из выпадающего списка, к которому у Пользователя есть доступ. Например, если компания Пользователя «А», то Пользователю будут доступны бренды «А.Карты», «А.Музыка» и т.п.

С помощью поисковой строки Пользователь может произвести поиск по виджету «Обнаруженные ресурсы». При вводе ключевых слов виджет покажет результаты, содержащие ключевые слова.

Кнопка «**Сгенерировать отчет**» позволяет Пользователю сформировать отчет с учетом заданных настроек. Все поля являются обязательными к заполнению.

Поле	Описание
Бренд	Необходимо выбрать бренд из выпадающего списка
Период	Укажите временной диапазон для сбора отчета. Чем шире диапазон - тем больше времени потребуется на формирование отчета
Часовой пояс	Можно выбрать часовой пояс, отличный от установленного в профиле
Язык	Выберите язык для отчета
Формат	Выберите расширение файла для отчета
Добавить таблицу XLSX с результатами	Пользователь получит ZIP-архив, в котором будет находиться отчет в выбранном формате и XLSX-таблица с данными из Системы

Нажмите кнопку «**Сгенерировать**», начнется процесс формирования отчета.

Не закрывайте окно, пока не начнется загрузка отчета на ваше устройство!

3.2 Нарушения

В разделе **Нарушения** представлена информация обо всех обнаруженных ресурсах, содержащих нелегитимное использование бренда или интеллектуальной собственности компании. Такие нарушения представлены в Системе в виде объектов, состоящих из пары бренд-ссылка (доменное имя). Данный раздел содержит структурированный список таких объектов. Отображение списка может быть настроено в соответствии с целями при помощи кнопки «**Выбор группировки**». В выпадающем списке можно выбрать один из видов:

- Просмотр скриншота;
- Стандартный;
- По домену;
- По хостингу;
- По регистратору.

. По умолчанию установлен вид – «Просмотр скриншота», который содержит следующую информацию:

- Последний снятый скриншот ресурса;
- Участники доменного процесса: хостинг-провайдер, регистратор и регистрант;
- Дата текущего статуса;
- Статус;
- Тип нарушения;
- Бренд компании;
- Ссылка;
- Источник;
- Согласование.

3.2.1 Фильтры в разделе

Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию с помощью фильтров:

- Статус – фильтрация по статусу нарушения;
- Тип – фильтрация по типу нарушений;
- Бренд – данные для выбранного бренда, из доступных Пользователю;
- Дата текущего статуса – фильтрация данных по статусу объекта;
- Старт-конец – данные за указанный период времени;
- - все фильтры.

При нажатии кнопки откроется окно с расширенным выбором фильтров. Выбранный набор фильтров можно сохранить в шаблон с помощью кнопки «**Сохранить текущий**

пресет» или использовать существующий шаблон из выпадающего списка под заголовком «Пресеты».

По умолчанию существует пресет (шаблон) **TypoSquatting**. Термин **TypoSquatting** относится к деятельности, связанной с регистрацией доменов, схожих по написанию с доменами оригинальных брендов, и использованием их в недобросовестных целях. При выборе этого пресета отобразятся все такие нарушения, обнаруженные Системой.

3.2.2 Экспорт данных

Для экспорта текущей выборки (с учетом примененных фильтров) в формате .CSV нажмите кнопку и выберите один из доступных вариантов:

Опция	**Описание**
Стандартный	Все поля без технических спецификаций: тип нарушения, дата, источник, ссылка
С комментариями	Тот же набор с комментариями к объектам
Расширенный	Все переходы между статусами и дополнительные технические поля описания объекта
Расширенный с комментариями	Тот же набор с комментариями к объектам
Расширенный со скриншотами	Тот же набор со скриншотами к объектам

3.2.3 Работа с нарушениями

При обнаружении нового ресурса с признаками нарушения Система присваивает такому ресурсу статус «**Обнаружено**». Все ресурсы с таким статусом попадают в раздел **Нарушения**.

Обработка одного ресурса

1. Перейдите в раздел **Нарушения** -> вкладка **Требуется согласование**.
2. Для удобства работы можно выбрать источник мониторинга и/или применить фильтры.
3. Нажмите на нужный элемент в списке. Откроется всплывающая боковая панель с подробной информацией о ресурсе и нарушении, которое содержится на данной ресурсе. Ознакомьтесь с нарушением.

4. На панели действий выберите один из статусов согласования:

Статус	Описание
Реагирование подтверждено	Ресурс содержит нарушение и должен быть принят в работу.
Отклонено	Ресурс не содержит нарушений. Реагирование на ресурс не требуется.
Официальный	Ресурс принадлежит клиенту или партнеру. Ресурсу присваивается статус **Легальный**, дальнейший мониторинг по ссылке производиться не будет.

5. Нажмите кнопку «**Подтвердить**».

Массовые действия

Для одновременной обработки нескольких нарушений можно использовать функцию массовых действий.

1. Перейдите в раздел **Нарушения** -> вкладка **Требуется согласование**.
2. Для удобства работы можно выбрать источник мониторинга и/или применить фильтры.
3. С помощью чекбокса выделите необходимые ресурсы. В панели действий выберите статус согласования.
4. Нажмите кнопку «**Подтвердить»**.

Быстрый режим

В разделе Нарушения доступен **Быстрый режим**, который позволяет обрабатывать ресурсы один за другим в виде ленты. Для перехода в Быстрый режим выполните следующие действия:

1. Перейдите в раздел **Нарушения** -> вкладка **Требуется согласование**.
2. В панели с быстрыми фильтрами нажмите кнопку «**Быстрый режим»**. Откроется всплывающая панель Быстрого режима.
3. Настройте фильтры (при необходимости) в верхней ленте панели с помощью кнопки .
4. Ознакомьтесь с нарушением. На панели действий выберите один из предложенных статусов и нажмите кнопку «**Сохранить**». Вы автоматически перейдете к следующему ресурсу.
5. По окончанию работы нажмите кнопку «**Выйти из быстрого режима**».