ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Attack Surface Management»

Руководство по установке и эксплуатации ПО

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Описание
ВПО	Вредоносное программное обеспечение
Домены	Символьное имя, служащее для идентификации областей, которые являются единицами административной автономии в сети Интернет, в составе вышестоящей по иерархии такой области
Заказчик	Лицо, которое использует на законных основаниях ПО на основании заключенного договора
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ» • Компанией-интегратором, по выбору Заказчика
ПО	Программное обеспечение «F6 Attack Surface Management»
Разработчик	АО «БУДУЩЕЕ»
Угроза	Потенциально возможное происшествие, преднамеренное или нет, которое может оказать нежелательное воздействие на систему и/или хранящуюся информацию.
API (Application Programming Interface)	Программный интерфейс, то есть описание способов взаимодействия одной компьютерной программы с другими.
MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)	Руководство по классификации и описанию кибератак и вторжений. Вместо того, чтобы рассматривать результаты атаки, он определяет тактику, указывающую на то, что атака продолжается
SaaS (Software as a Service)	Модель обслуживания, при которой программное обеспечение размещено в облачной инфраструктуре
SSH (Secure Shell)	Сетевой протокол, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL (Secure Sockets Layer)	Криптографический протокол, который использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений
SSO (Single Sign-On)	Метод аутентификации, который позволяет вам безопасно получать доступ к нескольким независимым сервисам и приложениям, используя один набор учетных данных

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Данный документ содержит руководство по установке и эксплуатации программного обеспечения «F6 Attack Surface Management» (далее — Система, ПО, Attack Surface Management, ASM).

1.2 Назначение ПО

«F6 Attack Surface Management» (ASM) — это комплексная информационно-аналитическая система, предназначенная для оценки поверхности атаки (цифровые активы в публичном доступе) компании Заказчика и связанных с ней третьих сторон.

Система обнаруживает активы в свободном доступе, оценивает уровень уязвимости таких активов и ранжирует их по уровню опасности, а также оповещает об активах с высоким уровнем риска для предотвращения потенциальной атаки. Для каждой найденной уязвимости Система предлагает рекомендации по исправлению.

2 НАЧАЛО РАБОТЫ

«F6 Attack Surface Management» 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

Для корректного функционирования ПО необходим веб-браузер.

ПО поддерживает работу на следующих версиях браузеров:

- Internet Explorer версии 8.0 и выше;
- Google Chrome версии 4.0 и выше;
- Mozilla Firefox версии 3.5 и выше;
- Apple Safari версии 4.0 и выше;
- Opera версии 10.5 и выше;
- iOS Safari версии 3.2 и выше;
- Opera Mobile версии 11.0 и выше;
- Google Chrome for Android версии 11.0 и выше;
- Mozilla Firefox for Android версии 26.0 и выше;
- Internet Explorer Mobile версии 10.0 и выше;
- Яндекс.Браузер версии 20 и выше;
- Microsoft Edge версии 105 и выше.

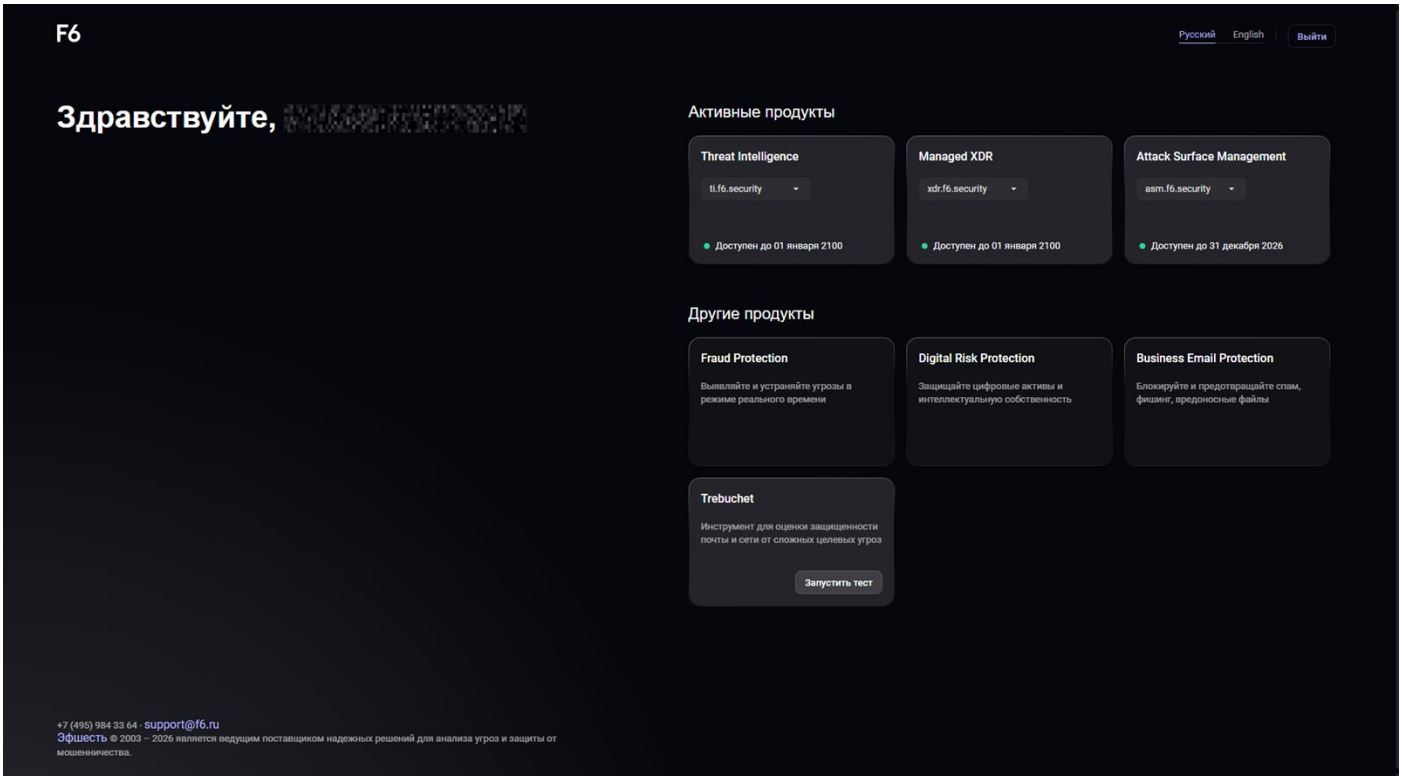
Требования для работы ПО с помощью API-интерфейса:

- Python 3.5.3.

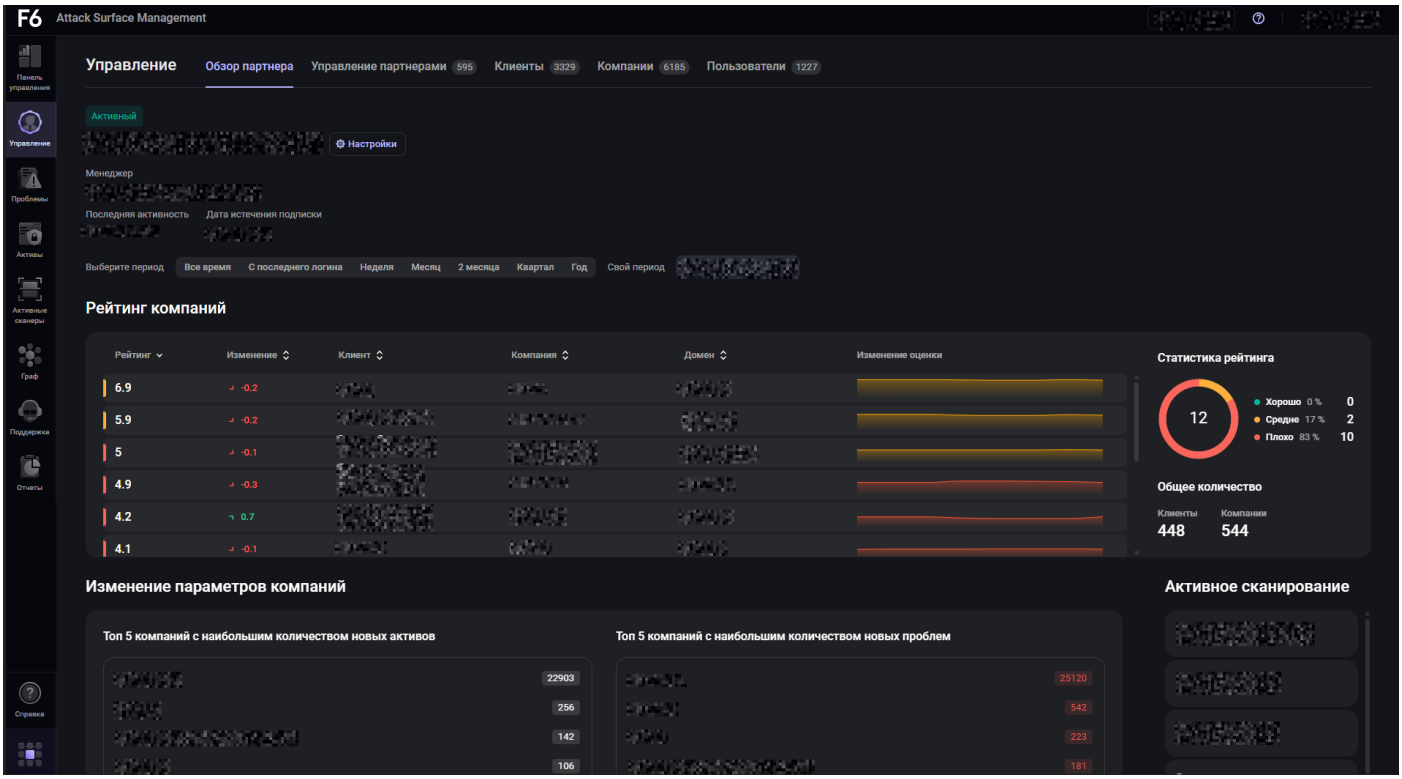
2.2 Вход в учетную запись

Для начала работы с ПО выполните следующие действия:

1. Откройте веб-браузер и перейдите по ссылке https://asm.f6.security/. Откроется страница авторизации.



2. Введите логин и пароль в соответствующие поля.
3. Нажмите на кнопку «**Войти**». После успешной авторизации отобразится страница раздела **Управление** ПО.



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

2.3 Доступ к ПО с помощью API-интерфейса

Доступ к системе предоставляется через Веб или API интерфейсы. Доступ к Веб-интерфейсу доступен всем клиентам. Доступ через API-интерфейс предоставляется после генерации API ключа.

Чтобы сгенерировать API-ключ перейдите в интерфейс Системы и выполните следующие шаги:

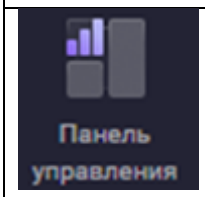
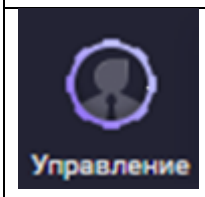
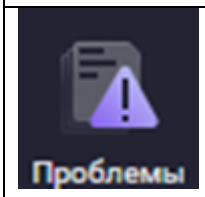
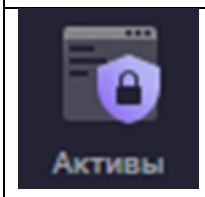
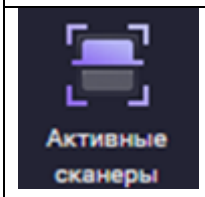
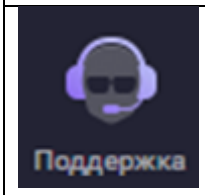
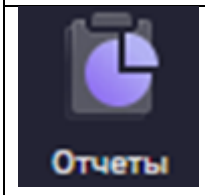
1. Перейдите на страницу https://asm.f6.security/info/api;
2. Нажмите кнопку «**Сгенерировать API ключ**» в правом верхнем углу страницы;
3. Откроется форма для генерации ключа. Введите пароль от вашей учетной записи;
4. Скопируйте созданный ключ с помощью кнопки «**Скопировать токен**». Сохраните ключ в хранилище паролей.

Внимание! Не передавайте ключ третьим лицам!

5. Авторизуйте ключ: нажмите кнопку «**Authorize**» в правом верхнем углу страницы. В появившейся форме введите скопированный ключ в поле «*value*». Нажмите кнопку «**Authorize**».

3 ИНТЕРФЕЙС ПО

Работа с ПО представляет собой взаимодействие с пользовательским интерфейсом ПО. Все разделы интерфейса доступны в боковой панели.

Раздел		Описание
	Панель управления	Главная страница ПО. Содержит виджеты с различными данными и статистикой
	Управление	Раздел содержит информацию о компании Заказчика, партнерах и клиентах
	Проблемы	Раздел содержит информацию об актуальных для компании Заказчика проблемах
	Активы	Раздел содержит информацию об активах Заказчика
	Активные сканеры	Раздел предназначен для инвазивного поиска и сбора информации о цифровых активах и киберугрозах
	Граф	Раздел предназначен для исследования как инфраструктуры злоумышленника, так и изучения собственной инфраструктуры извне (из сети Интернет) для выявления имеющихся или вероятных угроз
	Поддержка	Раздел позволяет просмотреть уже созданные заявки в Техническую Поддержку, а также оставить новую заявку
	Отчеты	В разделе содержатся отчеты пользователей

Далее будет описана работа с ключевыми разделами ПО.

3.1 Личный кабинет пользователя

Чтобы перейти в личный кабинет пользователя, нажмите на имя пользователя в правом верхнем углу страницы – **Профиль**. Откроется боковая всплывающая панель с личным кабинетом. В разделе **Профиль** доступны следующие действия:

– Просмотр информации о пользователе;

– Просмотр доступов;

– Просмотр журнала действий с учетной записью;

– Просмотр api журнала с информацией об api-ключах и действий с ними;

– Просмотр индивидуально созданных уведомлений и настройка уведомлений.

Информацию о пользователе можно изменить с помощью кнопки «**Редактировать**». Изменить можно:

– Язык Системы;

– Настройки уведомлений.

3.1.1 Настройка уведомлений

Во вкладке **Уведомления** можно настроить индивидуальные уведомления по интересующим объектам:

1. Нажмите кнопку «Редактировать» в правом верхнем углу. После нажатия появится кнопка «Добавить новое уведомление» в середине всплывающей панели. Откроется панель для создания уведомления.
2. Заполните пошаговую анкету для формирования уведомлений.
3. В конце нажмите кнопку «Сохранить», чтобы применить настройки уведомлений.

3.2 Панель управления

Раздел **Панель управления** представляет собой виджеты, на которых отображается следующая информация:

Виджеты	Описание
Ваша оценка	Оценка защищенности внешней поверхности атаки по данным ASM и медианная оценка по индустрии
Последние изменения	Динамика по видам проанализированных ASM данных
Динамика оценок по категориям	Оценка рисков по отдельным категориям
Карта активов	Графическое представление местонахождения активов на мировой карте

3.3 Управление

В разделе **Управление** представлена информация о компании Пользователя, клиентах, компании и пользователях. Раздел поделен на вкладки:

Вкладка	Описание
Клиенты	Список клиентов компании
Компании	Список доступных компаний
Пользователи	Список пользователей, относящихся к компании

3.3.1 **Клиенты**

Во вкладке **Клиенты** представлен список клиентов в виде карточек с информацией о:

- Статусе лицензии;
- Последней активности, дате истечения лицензии;
- Менеджере Разработчика;
- Количестве активов в лицензии;
- Индустрии;
- Стране.

При нажатии на выбранную карточку клиента откроется всплывающая боковая панель с подробной информацией о клиенте. В панели возможно просмотреть журнал действий с клиентом, а также просмотреть список пользователей клиента.

Для изменения информации о клиенте:

1. Нажмите на карточку клиента. Откроется всплывающая боковая панель.
2. Нажмите кнопку «Редактировать» в правом верхнем углу боковой панели.
3. Измените необходимые данные.
4. Нажмите кнопку «Сохранить».

3.3.2 **Компании**

Во вкладке **Компании** содержится информация о компаниях клиента. На главной странице вкладки представлена таблица со следующей информацией:

- Рейтинг (оценка безопасности);
- Компания;
- Клиент;
- Главный домен;
- Индустрия;
- Статус;
- Изменение оценки (отображена в виде статистики).

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

- Тип лицензии;
- Активное сканирование.

Для просмотра информации о компании нажмите на значок шестеренки. Откроется сплывающая боковая панель. В панели возможно просмотреть:

– Основную информацию о компании;
– Список доменов и IP-адресов, принадлежащих компании;
– Журнал действий;
– Настройки сканирования активов Системой;
– Автосортировка;
– Облачная инфраструктура компании.

Данные о компании можно отобразить на **Панели управления**. Для этого нажмите кнопку «Панель управления» в строке с нужной компанией. Откроется страница раздела **Панель управления** с данными о выбранной компании.

Для изменения информации о компании:

1. Нажмите на значок шестеренки в строке с нужной компанией. Откроется всплывающая боковая панель.
2. Нажмите кнопку «Редактировать» в правом верхнем углу боковой панели.
3. Выберите вкладку, данные из которой нужно изменить.
4. Измените необходимые данные.
5. Нажмите кнопку «Сохранить».

Для добавления новой компании:

1. Нажмите на кнопку «Добавить компанию». Откроется форма.
2. Заполните форму, добавьте главный домен, название компании, тип лицензии и индустрию.
3. Нажмите кнопку «Добавить».

3.3.3 **Пользователи**

Во вкладке **Пользователи** представлена информация о зарегистрированных в Системе пользователях, связанных с клиентом. Эти данные распределены по вкладкам в соответствии со статусом лицензии:

– Активные;
– Заблокированные;
– Удаленные;
– Все.

Данные представлены в виде карточек со следующей информацией:

– Статус лицензии;
– Имя пользователя;
– Электронная почта пользователя;
– Роль в Системе ASM;
– Клиент, к которому относится пользователь.

Для просмотра подробной информации о пользователе нажмите на карточку нужного пользователя. Откроется всплывающая боковая панель. Данные в панели разделены на вкладки:

Главное	**Детали выбранного пользователя**
Профиль	Контактные данные пользователя, название клиента и статус в системе ASM
Доступ	Данные о доступе к клиентам и партнерам
Журнал	Журнал действий, совершенных клиентами данной компании.
API журнал	Журнал обращений пользователя через API
Уведомления	Настройка уведомлений по проблемам, активам, клиентам, компаниям или партнерам

Для поиска нужного пользователя в разделе доступны поисковая строка и быстрый фильтр «Роль».

Для добавления новой компании:

1. Нажмите на кнопку «Добавить пользователя». Откроется форма.
2. Заполните форму: добавьте имя пользователя, электронную почту, выберите роль и клиента.
3. Нажмите кнопку «Добавить».

3.4 Проблемы

В разделе **Проблемы** представлена информация об обнаруженных недостатках. Эти данные распределены по вкладкам в соответствии со статусом проблемы:

Вкладка	Описание
Обнаруженные	Список всех проблем, которые были обнаружены, но еще не приняты в работу
В работе	Список проблем, которые были взяты в работу
Решенные	Проблема получит статус «Решено», если пользователь установит его вручную или если система определит, что проблема больше не обнаруживается в активах
Игнорируемые	При получении статуса «Игнорировать» сканирование актива продолжится, но проблема не будет влиять на оценку безопасности
Ложно-позитивные	Список проблем, которые были идентифицированы как проблемы ошибочно

Проблемы представлены в виде списка со следующей информацией:

– Тип проблемы (категория);

– Результат теста;

– Атрибуция по матрице MITRE ATT&CK;

– Связанный с проблемой актив;

– Путь на графе.

В каждой вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию при помощи фильтров:

– Категория – категория проблемы в Системе;

– Название теста – имя теста в Системе;

– Степень опасности – уровень опасности проблемы;

– Активное сканирование – проблемы, выявленные активным сканированием;

– Теги.

В каждой вкладке раздела **Проблемы** доступна выгрузка CSV-файлов с помощью кнопки загрузки.

Для просмотра подробной информации о проблеме нажмите на нужный элемент в списке. Откроется всплывающая боковая панель. Во вкладке «Основная информация» представлены следующие данные:

– Первое и последнее появление проблемы, активность в днях;

– Компания;

– Категория теста;

– Тип проблемы;

– Актив, связанный с проблемой;

– Результат теста;

– Контекст к проблеме (потенциальная опасность проблемы);

– Атрибуция проблемы по матрице MITRE ATT&CK.

Для категории проблем «DNS и домены» доступна ручная проверка. Команда для ручной проверки проблемы указана в строке «Как проверить» во всплывающей боковой панели. При нажатии команда автоматически копируется в буфер обмена. Далее ее можно вставить в терминал на вашем ПК для ручной проверки.

Обратите внимание: Команды рассчитаны только для ОС на базе UNIX.

Во вкладке «История действий» представлен журнал действий с проблемой (смена статусов в Системе, комментарии).

Для добавления комментария к проблеме:

1. Откройте всплывающую боковую панель с подробной информацией о проблеме.
2. Перейдите во вкладку «История действий».
3. В поле «Добавить комментарий» введите текст комментария.
4. Нажмите кнопку «Добавить».

3.5 Активы

В разделе **Активы** предоставлена информация о цифровых объектах Заказчика. Эти данные распределены по следующим вкладкам:

– Домены;

– SSL;

– IP-адреса;

– IP-подсети;

– Программное обеспечение;

– Логин формы,

– Тайпосквоттед домены.

Также информация во всех вкладках раздела Активы поделена на подразделы:

– Новые;

– Лишние или игнорируемые;

– Подтвержденные;

– Все.

В каждой вкладке раздела **Активы** доступна поисковая строка, а также выгрузка CSV-файлов с помощью кнопки загрузки.

3.5.1 Вкладка Домены

Во вкладке **Домены** содержится информация об обнаруженных доменах, имеющих связь с основными указанными доменами клиента. На главной странице вкладки представлены карточки со следующей информацией:

– Дата обнаружения домена;

– Дата последнего проведенного сканирования;
– Дата последнего взаимодействия с доменом;
– Имя домена;
– Дата регистрации домена;
– Дата окончания регистрации домена;
– Название регистратора;
– Электронный почтовый адрес, на который зарегистрирован домен;
– Компания, которой принадлежит домен;
– Имя владельца домена (может быть защищено правами приватности);
– Надежность домена по оценке Платформы;
– Обнаружен – информация о домене получена либо при помощи работы функциональности Платформы, либо путем обогащения из других источников.

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

– Основной домен - домен, указанный Клиентом как основной;
– Тип домена - ранжирование доменов;
– Регистратор - канал, через который зарегистрирован домен Клиента;
– Теги - метки для поиска данных Клиентом;
– Начало-конец – данные за указанный период времени;
– Обнаружение - способ обнаружения доменов Клиента;
– Наличие проблем - оценка проблем Клиента с помощью соответствующей градации;
– Шаги на графе - количество шагов до основного домена Клиента.

3.5.2 **Вкладка SSL**

Во вкладке **SSL** содержит в себе информацию обо всех обнаруженных сертификатах, имеющих связь с основными указанными доменами Клиента. На главной странице вкладки представлены карточки со следующей информацией:

– Дата обнаружения сертификата SSL;
– Дата последнего проведенного сканирования;
– SSL отпечаток;
– Валиден с;
– Валиден до;
– Общее имя;
– Компания, которой принадлежит данный сертификат;
– Эмитент;
– Надежность сертификата по оценке Платформы;
– Обнаружен - информация о сертификате получена либо при помощи работы функциональности Платформы, либо путем обогащения из других источников.

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

– Эмитент – компания, выпускающая сертификаты;
– Общее имя – название сертификатов одной группы;
– Теги;
– Начало-конец;
– Обнаружение – способ обнаружения сертификата;
– Наличие проблем;
– Шаги на графе.

3.5.3 **Вкладка IP-адреса**

Во вкладке **IP-адреса** собрана информация обо всех найденных IP-адресах, относящихся к Клиенту. На главной странице вкладки представлены карточки со следующей информацией:

– Дата обнаружения IP-адреса;
– Дата последнего проведенного сканирования;
– IP-адрес;
– Порты;
– Имя сети;
– Локация;
– Компания;
– Надежность IP-адреса по оценке Платформы;
– Обнаружен - информация об IP-адресе получена либо при помощи работы функциональности Платформы, либо путем обогащения из других источников.

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

– Локация;
– Автономная сеть;
– Имя сети;
– Открытый порт – номер порта входа;
– Теги;
– Обнаружение;
– Наличие проблем;
– Шаги на графе.

3.5.4 **Вкладка IP-подсети**

Во вкладке **IP-подсети** собрана информация обо всех IP-адресах, для удобства объединенных в группу подсетей. На главной странице вкладки представлены карточки со следующей информацией:

– Подсеть;
– Последнее сканирование;
– Имя сети;
– Локация;

– Автономная сеть;

– Компания;

– Порты.

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

– Локация;

– Автономная сеть;

– Имя сети;

– Открытый порт;

– Теги;

– Обнаружение;

– Наличие проблем;

– Шаги на графе.

3.5.5 **Вкладка Программное обеспечение**

Во вкладке **Программное обеспечение** собрана информация обо всех автоматически найденных на хостах экземплярах программного обеспечения с возможностью применения фильтров для обнаружения уязвимостей, самих продуктов и версии ПО. На главной странице вкладки представлены карточки со следующей информацией:

– Дата обнаружения;

– Последнее сканирование;

– Продукт;

– Версия;

– Тип ПО;

– Порт;

– Актив;

– Компания;

– Надежность;

– Уязвимости.

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

– Тип ПО – разновидность ПО, используемого в компании;

– Продукт – разновидность используемого продукта в компании;

– Порт;

– Уязвимости – тип уязвимости ПО;

– Теги;

– Обнаружение;

– Наличие проблем;

– Шаги в графе.

3.5.6 **Вкладка Логин формы**

Во вкладке **Логин формы** отображаются опубликованные в сети Интернет формы ввода логина и пароля, а также программное обеспечение, установленное на хостах. В этих формах могут быть как надежные пароли, так и стандартные несложные. На главной странице вкладки представлены карточки со следующей информацией:

- Дата обнаружения логин формы;
- Последнее сканирование;
- URL;
- Актив;
- Компания;
- Надежность;
- Программное обеспечение.

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

- Теги;
- Обнаружение;
- Наличие проблем;
- Шаги в графе.

3.5.7 **Вкладка Тайпосквоттед домены**

Во вкладке **Тайпосквоттед домены** содержится информация об опубликованных доменах, которые содержат преднамеренные орфографические неточности в доменном имени. На главной странице вкладки представлены карточки со следующей информацией:

- Дата обнаружения;
- Дата последнего проведенного сканирования;
- Тайпосквоттед домен;
- Исходный домен;
- HTTP статус;
- Редирект;
- Компания;
- Имя владельца тайпсквоттед домена (может быть защищено правами приватности);

Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию с помощью фильтра «Исходный домен».

3.6 Активные сканеры

Раздел **Активные сканеры** предназначен для поиска и сбора информации о цифровых активах и киберугрозах с целью их обнаружения и анализа. В разделе Активные сканеры представлены следующие вкладки:

- Брут;
- Фаззинг;
- Эксплойты;
- Сканирование портов.

3.6.1 **Брут**

Во вкладке **Брут** пользователю предоставляется информация о найденных уязвимостях, такие как пароли, которые могут быть подобраны по словарю. Чтобы получить эту информацию достаточно нажать на кнопку «Создать тест» и заполнить форму для выбранной компании. Результаты сканирования предоставляются в виде отчета. Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию, используя фильтры: по временному интервалу, активам, названию компаний и другим критериям.

3.6.2 **Фаззинг**

Во вкладке **Фаззинг** содержится информация об обнаруженных страницах с различным объемом контента. Процесс фаззинга позволяет выявить скрытые файлы и каталоги, а также проверить URL и HTTP-заголовки. Чтобы получить эту информацию достаточно нажать на кнопку «Создать тест» и заполнить форму для выбранной компании. Результаты сканирования предоставляются в виде отчета. Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию, используя фильтры: по временному интервалу, статус коду, типу страницы и другим критериям».

3.6.3 **Эксплойт**

Во вкладке **Эксплойт** осуществляется выполнение эксплойт-скриптов, которые используют уязвимости в системе клиента для выявления слабых мест. Чтобы получить информацию об уязвимостях достаточно нажать на кнопку «Создать тест» и заполнить форму для выбранной компании. Результаты теста отображаются в виде логов, сгенерированных эксплойтом. Если уязвимости не были обнаружены, то тестирование увенчалось успехом, в противном случае результат сканирования потребует проверки и анализа.

3.6.4 **Сканирование портов**

Во вкладке **Сканирование портов** осуществляется поиск открытых портов на устройствах, подключенных к сети, а также на серверах. Этот процесс позволяет автоматически проверять все шестьдесят пять тысяч портов на заданных IP-адресах, отображая только открытые порты и информацию об обнаруженных утилитах. Чтобы получить информацию об отсканированных портах достаточно нажать на кнопку «Создать тест» и заполнить форму для выбранной компании. Результаты сканирования предоставляются в виде отчета. Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию, используя фильтры: «Выбор временного диапазона», «Порт» и «Продукт».

3.7 Граф

Раздел **Граф** предназначен для исследования как инфраструктуры злоумышленника, так и собственной инфраструктуры извне (из сети Интернет) для выявления имеющихся или вероятных угроз.

С помощью графа можно отследить взаимосвязи между исследуемым активом и другими объектами. Активы представлены в графе в виде узлов, а соединяющие их отрезки обозначают связи. Перечень активов, доступных для исследования:

- Домены – узлы графа, связанные с доменным именем ресурса;
- IP-адреса – узлы графа, отражающие внешние IP-адреса, к которым привязаны домены;
- SSL-сертификаты – связанные с исследуемыми HTTPS-доменами сертификаты;
- SSH ключи – ключи, связанные с исследуемым хостом;
- Файлы – файлы, связанные с IP-адресами и доменными именами;

– Атрибуция – информация о ПО, обнаруженного на домене или IP-адресе;

– Emails – почтовые адреса, используемые при регистрации доменов;

– Контакты – карточки с контактами в виде телефонных номеров, emails, аккаунтов в соцсетях и т. д.;

– DarkWeb – карточки с активностью исследуемого актива в сети интернет.

Интерфейс графа состоит из следующих элементов:

– Меню выбора компании и домена;

– Граф;

– Панель с инструментами;

– Интерфейс всплывающей панели.

Интерфейс всплывающей панели содержит следующие категории: **Domains**, **IP**, **SSL**, **SSH**, **Files**, **Attribution**, **Contacts** и **DarkWeb**. Каждую из этих категорий можно раскрыть для получения дополнительной информации.

Категории — это активы, сгруппированные логически по вкладкам. Если во вкладке есть активы, то отобразится их количество, если активов нет, вкладка останется пустой.

Узлы графа имеют различные цвета в зависимости от их значения:

Цвет	Значение	Описание
Синий	Социальные сети	Ресурсы социальных сетей
Зеленый	Интернет	Сущности, связанные с сетью Интернет
Красный	Хакерская активность	Профили на специализированных форумах
Оранжевый	Вредоносная активность	Все сущности, связанные с вредоносным ПО
Голубой	Контактная информация	Перечисление контактных данных
Глициновый	Мессенджеры	Ресурсы мессенджеров
Пюсовый	Платформы	Ресурсы платформ

Данные графа можно отобразить за определенный период времени, используя настройку «Time period» в меню дополнительных настроек. Помимо этого, функциональными кнопками в правой панели возможно:

– Зафиксировать положение узлов графа (без движения);

– Сделать скриншот построенного графа;

– Вызвать окно спецификацию об узлах графа;

– Отобразить граф во весь экран.

В каждой вкладке раздела **Граф** доступна выгрузка CSV-файлов с помощью кнопки загрузки.

В выгруженном файле будут содержаться все данные из вкладки, которые включены в выборку. Данная выборка формируется пользователем самостоятельно при помощи фильтров.

Также есть возможность самостоятельного поиска активов с помощью поисковой строки.

3.8 Поддержка

Раздел **Поддержка** создан для оказания помощи пользователям в устранении проблем и поиске информации и содержит в себе следующие вкладки:

– Новые запросы – отображаются все недавно созданные тикеты, ожидающие обработки;

– В обработке – отображаются тикеты, взятые в работу, и их исполнители;

– Решенные – информация обо всех закрытых запросах.

– Все – полный архив запросов.

Для создания запроса:

1. Нажмите кнопку **Создать запрос** в правом верхнем углу
2. Выберите категорию запроса:

– Отчет об ошибке;

– Другое.

3. В описании опишите проблему. Предоставьте как можно больше информации для ускорения решения. При необходимости прикрепите файл.
4. В категории запроса «Другое» доступна опция «Временные ожидания». Пользователь может добавить дату дедлайна – крайнюю дату рассмотрения заявки специалистом Разработчика, а также отметить запрос как срочный с помощью чекбокса.

Для поиска нужного запроса доступна поисковая строка, а также быстрые фильтры:

– Мои;

– Посещенные;

– Срочные;

– Все команды – команды технической поддержки Разработчика;

– Проекты.

3.9 Отчеты

В разделе **Отчеты** вы можете создавать и планировать экспорт PDF-файлов.

Отчеты предназначены для отслеживания динамики вашей поверхности атаки, её общего обзора, а также работы с проблемами.

Отчеты делятся на 2 типа – Отчеты без расписания и Отчеты по расписанию. Также доступен полный список отчетов во вкладке Все отчеты. Каждому типу отведена отдельная вкладка.

Отчеты представлены в виде списка. Чтобы просмотреть отчет, нажмите на три точки – «Открыть отчет в новой вкладке».

Чтобы скачать отчет на устройство, нажмите три точки – «Скачать отчет». Файл автоматически загрузится на устройство.

Для поиска нужного отчета доступна поисковая строка, а также быстрые фильтры:

– Мои отчеты – персональные отчеты;
– Автор – отчеты конкретного пользователя;
– Получатели – отчеты выбранных получателей;
– Компания – отчеты по выбранной компании;
– Начало – Конец – отчеты за выбранный временной диапазон.

Для создания отчета:

1. Нажмите кнопку **Создать отчет**. Откроется форма для создания отчета.
2. Выберите клиента и компанию из выпадающего списка.
3. Выберите период, за который необходимо создать отчет. По умолчанию отчет создается за последние 30 дней.
4. Настройки отчета можно сохранить в шаблон - для этого установите чекбокс «Сохранить шаблон». Дайте название шаблону. Если необходимо, выберите функцию «Повторять по расписанию» и задайте периодичность автоматического создания отчета. Такие отчеты будут появляться во вкладке Отчеты по расписанию.
5. Выберите виджеты, которые необходимо добавить в отчет. При необходимости выберите техническое приложение, которое должно попасть в отчет.
6. Нажмите кнопку «Создать отчет». Когда отчет будет сформирован, вы получите уведомление на электронную почту.
7. Созданный отчет будет автоматически направлен на электронную почту, а также отобразится в разделе **Отчеты**.