ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Threat Intelligence»

Руководство по установке и эксплуатации ПО

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Описание
ВПО	Вредоносное программное обеспечение
Дамп	Информация с банковской карты, записанная в файл
Заказчик	Лицо, заключившее договор на использование ПО
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ»; • Компанией-интегратором, по выбору Заказчика
Кардшоп	Порталы, на которых мошенники торгуют данными банковских карт
ПО, F6 Threat Intelligence	Программа для ЭВМ «F6 Threat Intelligence»
Пользователь	Лицо, непосредственно использующее ПО
Разработчик	АО «БУДУЩЕЕ»
Сигнатура	Уникальный код, который ассоциируется с определенным документом, сообщением, программным обеспечением или любым другим объектом
Токен	Средство идентификации пользователя или отдельного сеанса работы в компьютерных сетях и приложениях
Угроза или Киберугроза	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 кибератаки, когда мошенники создают поддельные сайты, имитирующие реальные веб-ресурсы, чтобы украсть

Термин	Описание
	конфиденциальную информацию пользователей (например, учетные данные, данные банковских карт и т. п.)
Эксплойт	Подвид вредоносного ПО, способного воспользоваться уязвимостями в программном обеспечении для атаки на целевую систему
API (Application Programming Interface)	Программный интерфейс, то есть описание способов взаимодействия одной компьютерной программы с другими
CVE (Common Vulnerabilities and Exposures)	База данных известных уязвимостей и дефектов безопасности
CVSS (Common Vulnerability Scoring System)	Открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы, обычно с целью понять приоритет ее исправления
Darkweb (даркверб)	«Темная сеть», скрытая анонимная сеть интернета, где действуют злоумышленники, а также форумы в открытом Интернете, посвященные хакерской тематике
DDoS-атака (Distributed Denial of Service)	Атака, целью которой является перегрузка сетевых ресурсов, делая их недоступными для их законных пользователей
OSINT (Open Source Intelligence)	Разведка по открытым источникам. То есть сбор и анализ информации, полученной из разных общедоступных информационных каналов.
PoC (Proof-of-Concept)	Моделирование работы ПО или эксплойта с целью найти оптимальный способ защиты или возможность компрометации системы
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

Термин	Описание
TLP (Traffic Light Protocol)	Набор обозначений для маркировки конфиденциальной информации с целью указать аудиторию ее дальнейшего распространения
TOR (The Onion Router)	Свободное и открытое программное обеспечение, использующее технологию «луковой маршрутизации» (множественной цепочки маршрутов) — сети специальных нод, каждая из которых шифрует данные пользователя
TTP (Tactics, Technics, Procedures)	(Тактики, Техники, Процедуры). Набор тактик, техник и процедур, используемых злоумышленниками
VPN (Virtual Private Network)	Обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх чьей-либо другой сети

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит руководство по установке и эксплуатации «F6 Threat Intelligence».

1.2 Назначение ПО

«F6 Threat Intelligence» — это система киберразведки, предназначенная для сбора, анализа и распространения информации о событиях безопасности, киберугрозах и уязвимостях.

Система представляет собой обширную базу знаний, содержащую информацию по злоумышленникам, угрозам и возможным уязвимостям, а также предоставляет данные о вредоносном программном обеспечении. По выявленным событиям кибербезопасности Система генерирует оповещения.

Кроме того, в Системе представлены аналитические отчеты о последних киберугрозах, что позволяет выстроить наиболее эффективную защиту инфраструктуры.

2 НАЧАЛО РАБОТЫ

«F6 Threat Intelligence» 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:

- Windows 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;
- 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.

2.2 Создание учетной записи

Для доступа к ПО необходима учетная запись Пользователя Системы. Перед началом работы с ПО необходимо обратиться к сотрудникам 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 (Рисунок 1).

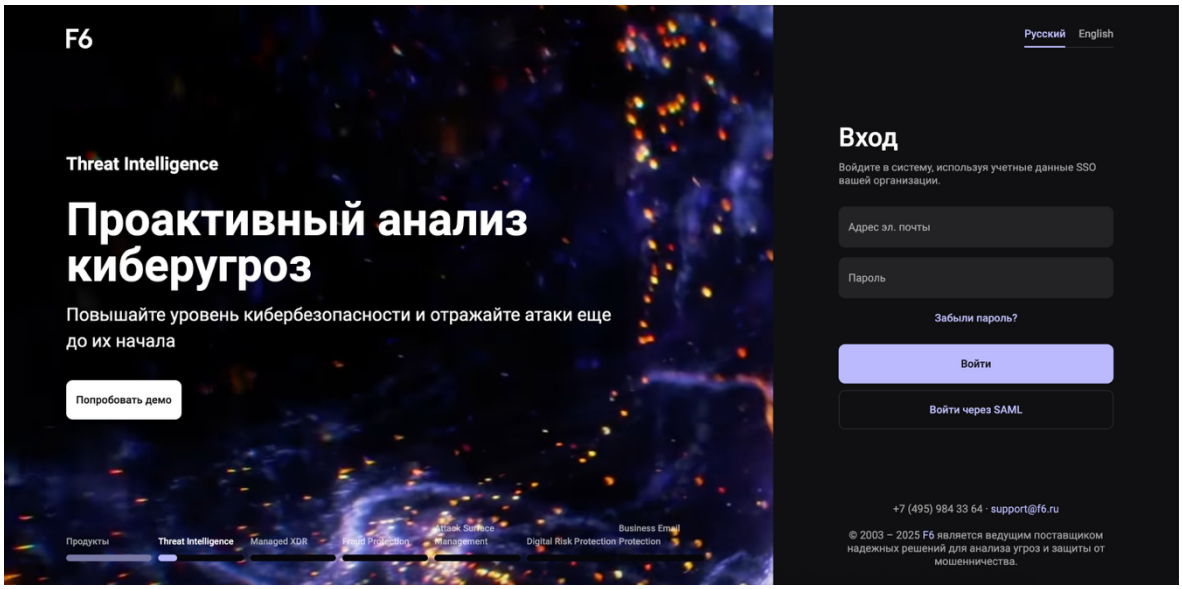


Рисунок 1. Страница авторизации

2. Введите логин и пароль в соответствующие поля.
3. Нажмите кнопку **Войти**.
4. Выберите необходимое ПО (Рисунок 2).

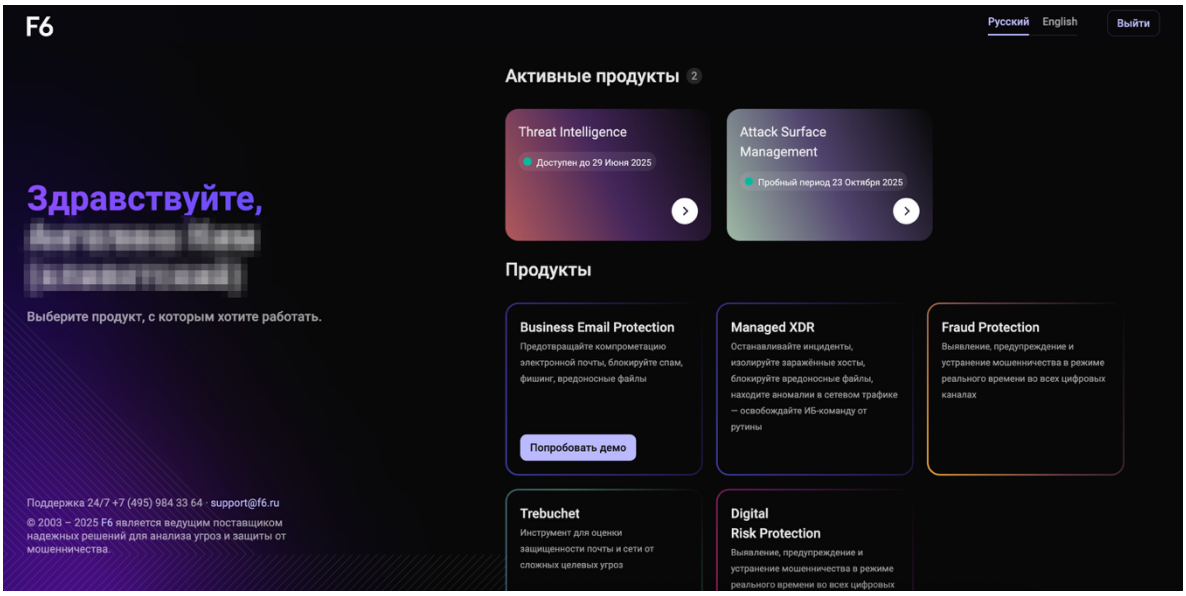


Рисунок 2. Главная страница SSO

После успешной авторизации отобразится главная страница «F6 Threat Intelligence» (Рисунок 3).

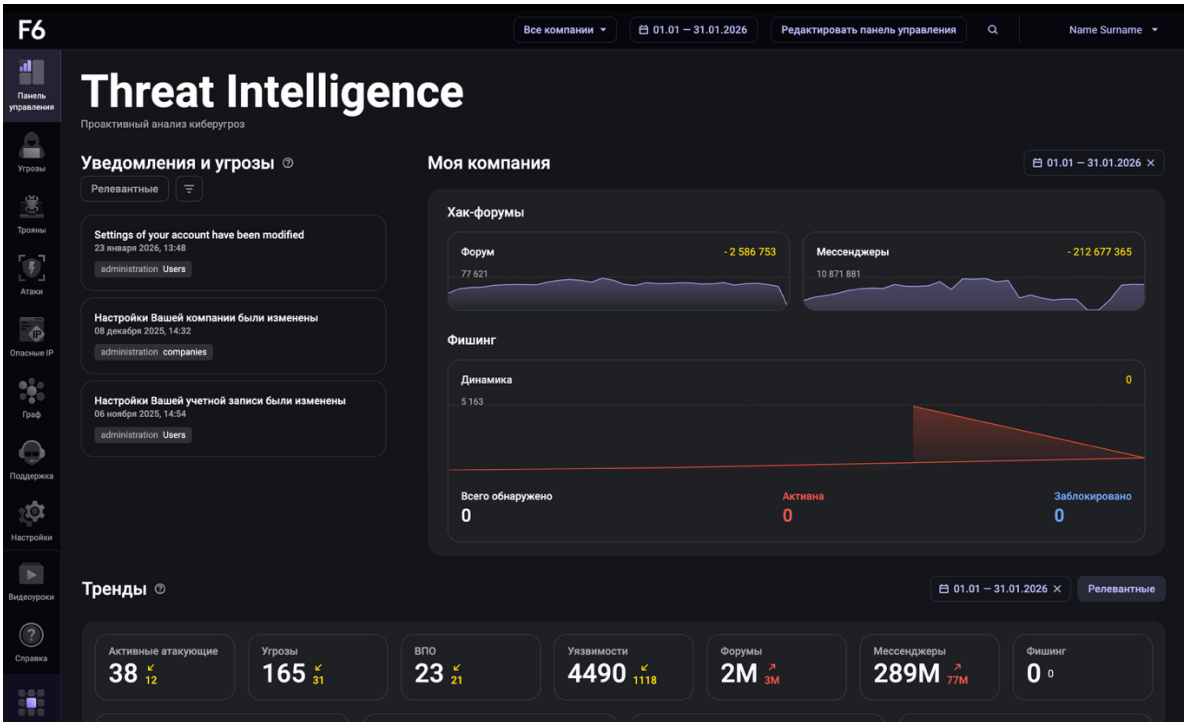


Рисунок 3. Главная страница ПО

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

2.4 Доступ к ПО с помощью API-интерфейса 1.0

API 1.0 — программный интерфейс для получения данных, предназначенный для интеграции «F6 Threat Intelligence» с системами внутренней безопасности и защиты Заказчика от мошеннических действий. API 1.0 использует протокол RESTful. Данные возвращаются в формате JSON.

Для доступа к API-интерфейсу 1.0 необходимо:

1. Предоставить ваши публичные IP-адреса, чтобы Разработчик внес их в список разрешенных адресов для доступа к API.
2. Войти в свою учетную запись (см. **2.3 Вход в учетную запись**), сгенерировать и сохранить API-ключ в вашем Профиле (см. **2.4.1 Генерация API-ключа**).
3. Внести следующие IP- и URL-адреса в список доступа своих систем внутренней безопасности.

IP-адреса	URL-адреса
46.148.232.87 84.38.187.26 87.249.58.4 212.41.13.86 212.41.13.102 31.184.219.128	ti.f6.security (для доступа к веб-порталу и API) sso.f6.security (требуется для доступа к интерфейсу) servicedesk.f6.security (требуется для доступа к интерфейсу) matrix.f6.security (требуется для доступа к интерфейсу) element-web.f6.security (требуется для доступа к интерфейсу)

2.4.1 Генерация API-ключа

Чтобы сгенерировать API-ключ, перейдите в интерфейс системы TI и выполните следующие шаги:

1. Перейдите на страницу https://ti.f6.security/.
2. Кликните на свое имя в правом верхнем углу и выберите **Личный кабинет**.
3. Перейдите во вкладку «Безопасность и доступ», затем нажмите **Персональный токен**.
4. Нажмите кнопку **Создать токен** (Рисунок 4).

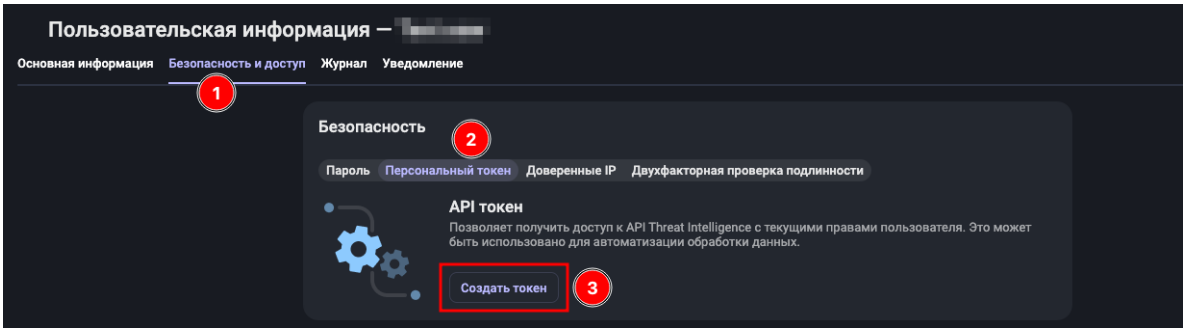


Рисунок 4. Создание API-ключа

5. Введите пароль. Скопируйте сгенерированный API-ключ и нажмите **Сохранить**, чтобы сохранить все изменения (Рисунок 5).

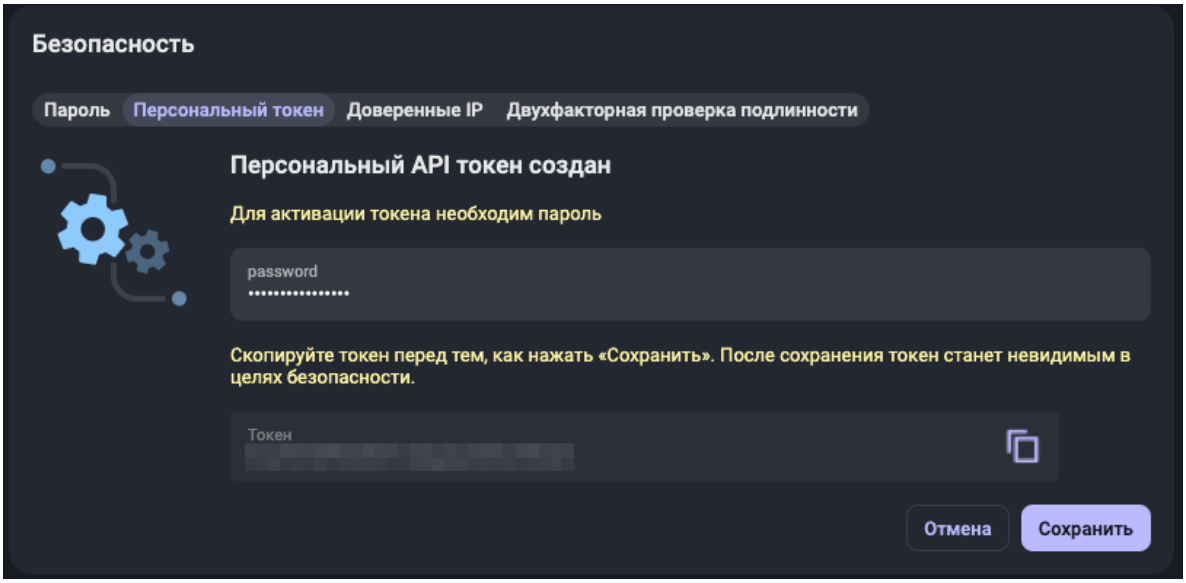


Рисунок 5. Сохранение API-ключа

***Примечание**. Не забывайте сохранять все изменения во время генерации API-ключа!*

2.5 Доступ к ПО с помощью API-интерфейса 2.0

API 2.0 — модификация API-интерфейса 1.0, в которой реализована функциональность подсчета количества обращений к БД ПО «Threat Intelligence» и полученных данных. API 2.0 использует протокол RESTful. Данные возвращаются в формате JSON.

Для доступа к API-интерфейсу 2.0 необходимо выполнить следующие шаги:

1. Авторизуйтесь в интерфейсе ПО по адресу https://sso.f6.security/ (см. **2.3 Вход в учетную запись**)
2. Выберите ПО «Threat Intelligence» (Рисунок 6).

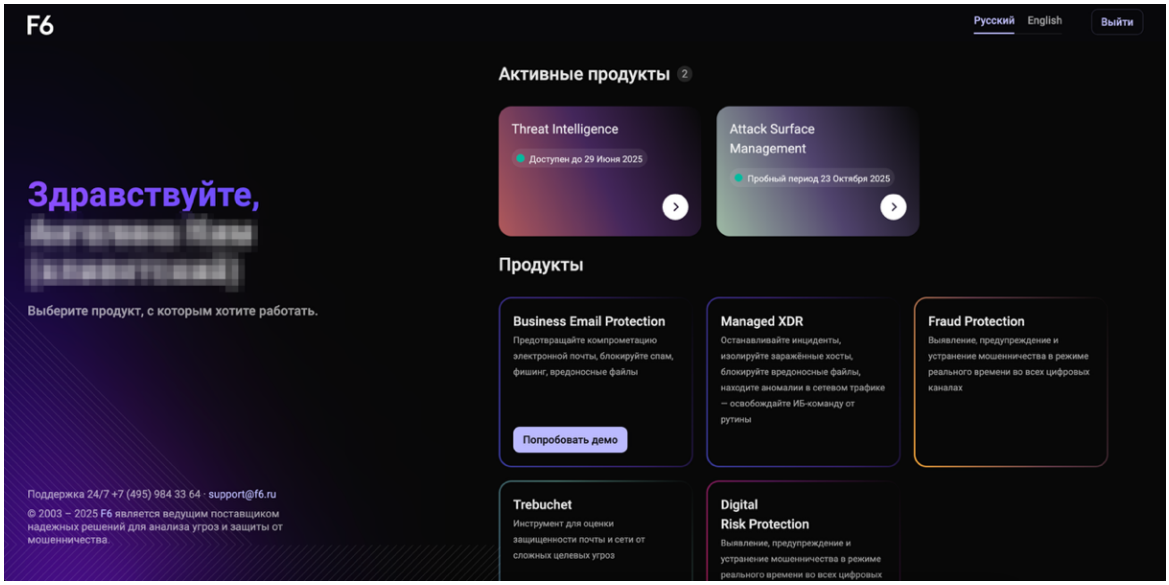


Рисунок 6. Главная страница SSO

После успешной авторизации отобразится главная страница веб-интерфейса API 2.0 (Рисунок 7).

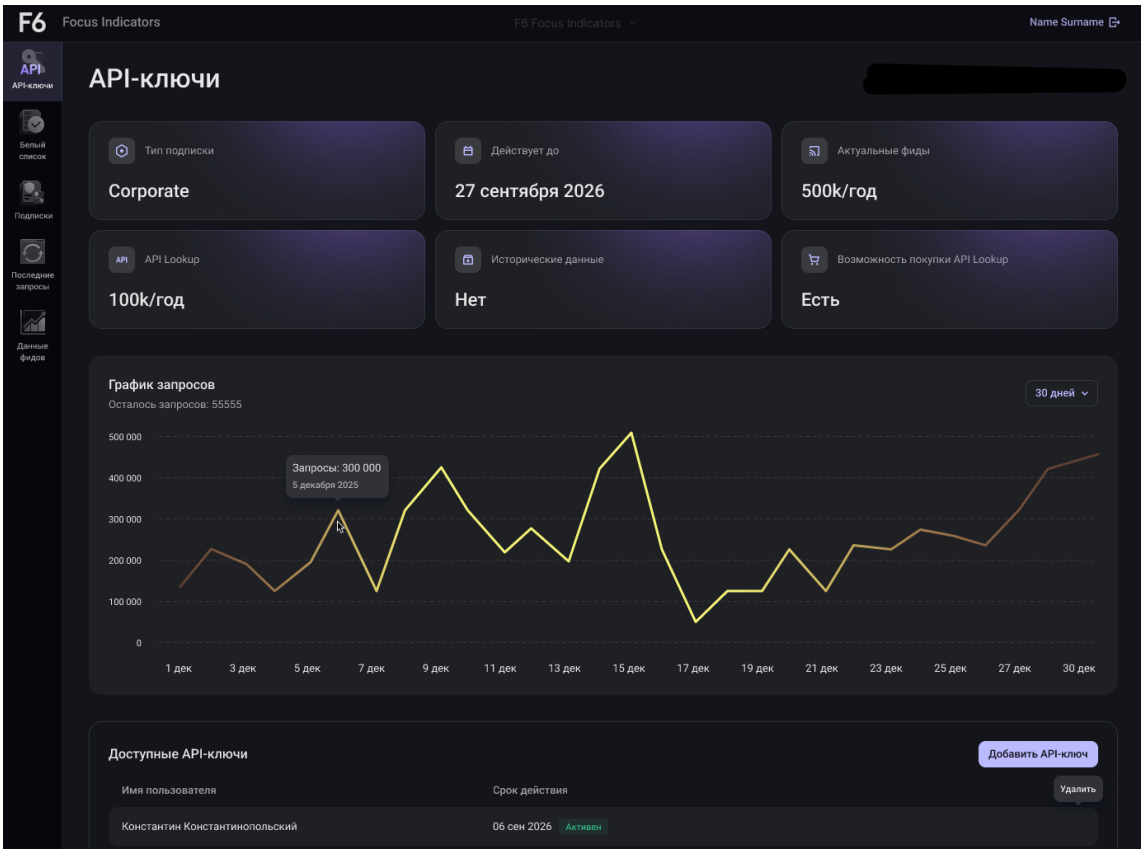
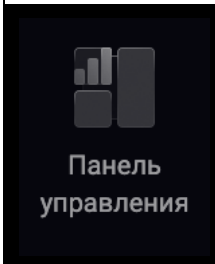
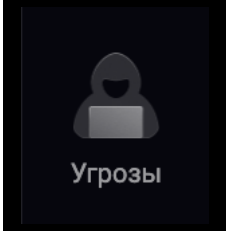
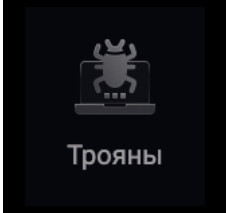
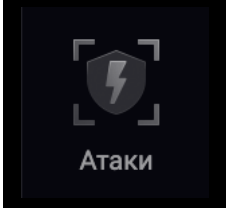
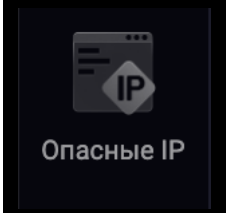


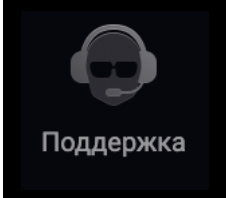
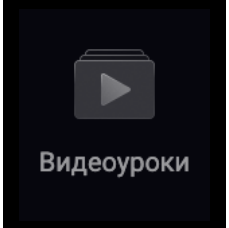
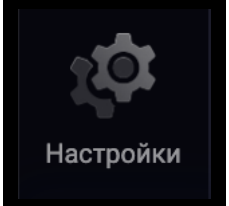
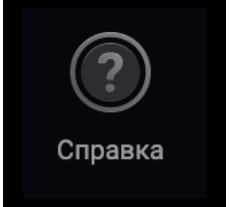
Рисунок 7. Главная страница веб-интерфейса API 2.0

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

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
	Угрозы	Раздел содержит информацию о самых актуальных угрозах кибербезопасности и злоумышленниках (группах злоумышленников), а также аналитические отчеты
	Трояны	Раздел содержит информацию о вредоносном ПО, которое было обнаружено в процессе анализа активности злоумышленников
	Атаки	Раздел содержит информацию о последних совершенных кибератаках и ресурсах, на которые были совершены эти атаки
	Опасные IP	Раздел содержит информацию об опасных IP-адресах, используемых злоумышленниками
	Граф	Раздел предназначен для визуализации связей между инфраструктурой злоумышленников, индикаторами компрометации и компрометированными данными в виде графа с узлами

Раздел		Описание
	Поддержка	Раздел позволяет просмотреть уже созданные заявки в Техническую Поддержку, а также оставить новую заявку
	Видеоуроки	В разделе доступны видеоуроки по использованию ПО
	Настройки	В разделе осуществляются общие настройки для всех пользователей, а также настройки конфиденциальности и безопасности
	Справка	Раздел содержит документацию к ПО, соглашения и лицензии

Далее будет описана работа с ключевыми разделами ПО.

3.1 Панель управления

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

Виджет	Описание
Уведомления и угрозы	Все релевантные данные для компании Пользователя
Моя компания	Релевантные для компании Пользователя данные о группировках злоумышленников
Тренды	Релевантные для компании Пользователя данные о последних трендах киберугроз и атак
Выявлено фишинга	Выявленные фишинговые атаки и их статусы, а также статистика по выявленным фишинговым атакам
Статистика фишинга	

Виджет	Описание
Найдено банковских карт	Данные о продаже банковских карт и дампов, а также статистика по их продаже
Статистика банковских карт	
Матрица MITRE ATT&CK	Описание и категоризация данных о группировках злоумышленников по матрице MITRE ATT&CK
Анализ и статистика вредоносного ПО	Данные об обнаруженным вредоносным ПО и статистика

3.1.1 Действия с Панелью управления

Панель управления можно редактировать: виджеты возможно добавлять, удалять и перемещать на панели. Для этого необходимо нажать кнопку **Редактировать панель управления** в верхней строке. Откроется всплывающее окно с редактированием виджетов.

Виджеты «Уведомления и угрозы» и «Моя компания» удалить и переместить нельзя, они всегда будут расположены в начале Панели. Остальные виджеты можно:

1. Менять местами — для этого нужно перетащить виджет или использовать кнопки управления в левой боковой панели виджета;
2. Удалять — для этого нужно нажать кнопку **Удалить** в верхнем правом углу виджета;
3. Добавлять — для этого нужно пролистать до конца всплывающего окна и добавить необходимые виджеты с помощью кнопки **Добавить виджет**.

3.2 Угрозы

В разделе **Угрозы** представлена информация о самых актуальных угрозах кибербезопасности и злоумышленниках (группах злоумышленников), а также аналитические отчеты. Эти данные разделены по вкладкам:

- Атакующие;
- Последние угрозы;
- Хак-форумы;
- Открытые угрозы;
- Мессенджеры;
- Ландшафт угроз;
- Аналитические отчеты.

3.2.1 Атакующие

Во вкладке **Атакующие** представлена информация о злоумышленниках и совершенных ими атаках. На главной странице представлены карточки всех опубликованных атак со следующей информацией:

- Имя атакующего (или группы), а также другие возможные псевдонимы;
- Первая и последняя зафиксированная активность группировки;
- Страна, из которой группировка ведет свою деятельность;
- Отрасль, ставшая целью злоумышленника;
- География — страны, в которых группировка проявляла свою активность;
- Теги;
- Последние угрозы — информация о последних зафиксированных атаках группировки.

В нижней части карточки расположена кнопка **Добавить в Ландшафт угроз**, при помощи которой можно перенести группировку в раздел **Ландшафт угроз**.

При нажатии на карточку открывается всплывающее окно с подробным описанием группировки.

Также информация во вкладке **Атакующие** поделена на подразделы:

- **Все** — главная страница;
- **Гос. атакующие** — организованные группы в сфере высоких технологий, работающие на определенное государство;
- **Киберпреступники** — организованные преступные группы в сфере высоких технологий, нацеленные на различные сектора экономики и страны;
- **Правила для Threat Hunting** — карточки преступных групп, для которых специалистами Разработчика созданы автоматические правила детектирования сетевой инфраструктуры или новых атак.

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

- MITRE — фильтрация данных по матрице MITRE ATT&CK;
- Начало – Конец — данные за указанный период времени;
- Последнее появление/Первое появление — сортировка данных по последнему или первому появлению атакующих, по возрастанию или убыванию;
-  — все фильтры.

3.2.2 Последние угрозы

Во вкладке **Последние угрозы** представлена актуальная информация об опубликованных угрозах кибератак или уже совершенных атаках, отсортированная в хронологическом порядке, начиная с самых свежих. На главной странице представлен список со следующей информацией:

- Заголовок информации об угрозе или атаке;
- Имя атакующего (или группы);
- Дата публикации;
- Теги экспертизы;
- Оценка качества;
- Количество просмотров.

При нажатии на заголовок открывается всплывающее окно с подробным описанием угрозы или совершенной атаки.

Также информация во вкладке **Последние угрозы** поделена на подразделы:

- **Все** — главная страница;
- **Гос. атакующие** — организованные группы в сфере высоких технологий, работающие на определенное государство;
- **Киберпреступники** — организованные преступные группы в сфере высоких технологий, нацеленные на различные сектора экономики и страны;
- **Учетки от шифровальщиков** — информация, относящаяся к использованию шифровальщиков;
- **Правила для Threat Hunting** — карточки преступных групп, для которых специалистами Разработчика созданы автоматические правила детектирования сетевой инфраструктуры или новых атак.

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

- MITRE — фильтрация данных по матрице MITRE ATT&CK;
- Персональный — фильтр отображает отчеты об угрозах, направленных на конкретную компанию. Данные отчеты доступны только компании Пользователя и сотрудникам Разработчика;
- Начало – Конец — данные за указанный период времени;
- Дата публикации — сортировка данных по дате публикации, по возрастанию или убыванию;
-  — все фильтры.

3.2.3 Хак-форумы

Во вкладке **Хак-форумы** представлены сообщения из Darkweb-форумов злоумышленников. Изначально отображаются только релевантные данные для организации, но также доступен поиск по всему массиву имеющихся в Системе данных. На главной странице представлен список со следующей информацией:

- Дата и время обнаружения сообщения;
- Имя атакующего (или группы), доменное имя форума;
- Заголовок сообщения/ветки сообщений;
- Тело сообщения;
- Теги;
- Информация о сообщении:
    - Дата публикации первого и последнего сообщения;
    - Количество участников обсуждения;
    - Количество сообщений в ветке.

Действия с сообщениями из списка проводятся с помощью появляющихся кнопок в правой части сообщения:

Кнопка	Описание
	Показать ветку сообщений целиком. При нажатии отобразятся все сообщения из одной ветки обсуждения
	Скрыть сообщение
	Добавить сообщение в избранное

При нажатии на заголовок открывается всплывающее окно с подробной информацией о сообщении.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, для которых специалистами Разработчика созданы автоматические правила детектирования сетевой инфраструктуры или новых атак;
- Ник — фильтрация сообщений от одного или нескольких пользователей;
- Форум — данные с одного или нескольких форумов;
- Теги — данные по одному или нескольким тегам;
- Начало – Конец — данные за указанный период времени;
-  — все фильтры.

Также данные можно выгрузить в виде JSON-файла с помощью кнопки загрузки.

3.2.4 Открытые угрозы

Во вкладке **Открытые угрозы** представлены публичные отчеты о текущих угрозах информационной безопасности, собранные методом OSINT (Open Source Intelligence) из различных источников. Данные, содержащиеся в разделе, включают открытые источники различных поставщиков средств обеспечения кибербезопасности и публичные исследования. На главной странице представлен список со следующей информацией:

- Дата загрузки отчета в систему ПО;
- Ссылка на источник;
- Страны, которые охватывает отчет;
- Тема отчета, краткий отрывок из начала отчета;
- Теги;
- Последние угрозы, созданные атакующим.

Каждый из отчетов также отмечен меткой «severity», которая обозначается цветовым индикатором в левой части карты.

Цвет	Уровень «severity»	Описание
Зеленый	Низкий	Угроза, описанная в отчете, не нанесет ущерба.
Желтый	Средний	Угроза, описанная в отчете, в случае реализации вызовет значительные последствия.
Красный	Высокий	Угроза, описанная в отчете, в случае реализации нанесет значительный ущерб. Сообщения с таким уровнем «severity» требуют повышенного внимания.

При нажатии на строку открывается всплывающее окно с подробной информацией по отчету.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, для которых специалистами Разработчика созданы автоматические правила детектирования сетевой инфраструктуры или новых атак;
- Тип источника — фильтрует отчеты по источнику, в котором они были найдены;
- Атакующий — отображает только отчеты, относящиеся к определенному злоумышленнику. На этой вкладке есть возможность поиска по имени атакующего/атакующей группировки;
- Вредоносная программа — отображает только отчеты, относящиеся к определенному вредоносному ПО;

- Теги — данные по одному или нескольким тегам;
- Начало – Конец — данные за указанный период времени.
-  — все фильтры.

3.2.5 Мессенджеры

Во вкладке **Мессенджеры** представлена информация из каналов общения злоумышленников. На данный момент анализируются два источника: Telegram и Discord. На главной странице представлен список со следующей информацией:

- Дата публикации найденного сообщения;
- Название чата/канала;
- Тип источника (Telegram/Discord). Расположен под названием группы/чата;
- Имя отправителя сообщения;
- Первые 30–40 символов сообщения, в полном тексте которого либо содержится информация о вашей компании, либо в нем нашлось соответствие текущему поисковому запросу;
- Информация о сообщении:
    - Дата публикации первого и последнего сообщения;
    - Количество участников обсуждения;
    - Количество сообщений в ветке.

При нажатии на строку открывается всплывающее окно с информацией о чате/канале, в котором сообщение было обнаружено. Для удобства просмотра интерфейс в этом окне приближен к реальному виду чата/канала в мессенджере.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, для которых специалистами Разработчика созданы автоматические правила детектирования сетевой инфраструктуры или новых атак;
- Скрыть спам — фильтр скрывает сообщения, отправленные ботами;
- Начало – Конец — данные за указанный период времени;
- Дата — сортировка данных по дате загрузки данных в платформу ПО, по возрастанию или убыванию;
-  — все фильтры.

С помощью кнопки **Добавить источник** Пользователь может добавить интересующий его ресурс на мониторинг. При нажатии на кнопку открывается всплывающее окно с формой для добавления ресурса:

- Тип — необходимо выбрать тип источника (Telegram/Discord);

- Ссылка — необходимо вставить URL-ссылку на источник;
- Комментарий — заполняется по желанию.

3.2.6 Ландшафт угроз

Во вкладке **Ландшафт угроз** можно выбрать интересующие или релевантные группировки злоумышленников для мониторинга их активности. Данные разделены по:

- компании;
- партнерам (компании-партнеры);
- отрасли;
- другие — раздел заполняется прикрепленным за Заказчиком аналитиком Разработчика.

Данные, добавленные с помощью кнопки **Добавить в Ландшафт угроз** во вкладке **Атакующие**, отобразятся здесь.

Также можно добавить интересующую группировку с помощью кнопки **+**. При нажатии на кнопку появится выпадающий список с названиями группировок, из которого необходимо выбрать нужную группировку или ввести название группировки.

3.2.7 Аналитические отчеты

Во вкладке **Аналитические отчеты** формируются ежемесячные, ежеквартальные, годовые отчеты об известных случившихся инцидентах, трендах злоумышленников и персонализированные отчеты для Заказчика.

Также формируются отчеты по конкретным угрозам и сложном вредоносном ПО, отчеты о готовящихся атаках на клиентов, содержащие подробную информацию об активности, индикаторах, артефактах по вредоносному объекту, а также рекомендации по противодействию.

На главной странице представлен список отчетов со следующей информацией:

- Дата публикации отчета;
- Обложка отчета;
- Тема отчета, страна публикации, первые 120–130 символов отчета;
- Наименование компании, опубликовавшей отчет;
- TLP - ранжирование данных по протоколу TLP.

При нажатии на выбранный отчет загружается полный документ по нему.

Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также найти отчеты за указанный период времени.

3.3 Трояны

Раздел **Трояны** содержит информацию о вредоносном ПО, которое было обнаружено в процессе анализа активности злоумышленников. Эти данные разделены по вкладкам:

- Отчеты;
- Детонация ВПО;
- Конфигурации;
- Фишинг комплекты;
- Уязвимости.

3.3.1 Отчеты

Во вкладке **Отчеты** представлена подробная информация о вредоносном ПО, которое было обнаружено в процессе анализа активности злоумышленников. На главной странице представлены карточки со следующей информацией:

- Платформа — операционные системы, которые были атакованы с помощью этого ВПО;
- Категория — тип ВПО;
- Атакующие группы;
- Связанное вредоносное ПО;
- Страны, в которых была замечена активность ВПО.

В нижней части карточки расположены кнопки «палец вверх» и «палец вниз» для оценки качества, а также показатель количества просмотров.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы.**

При нажатии на карточку открывается всплывающее окно с подробным описанием ВПО.

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

- Платформа — фильтрация по одному или нескольким операционным системам, которые были атакованы с помощью ВПО;
- Категория — данные по одному или нескольким типам ВПО;
- Страна — данные по одной или нескольким странам, в которых была замечена активность ВПО;
- Регион — данные о ВПО для определенного региона;
- MITRE — фильтрация данных по матрице MITRE ATT&CK.

3.3.2 Детонация ВПО

Во вкладке **Детонация ВПО** предоставляется доступ к системе **Malware Detonation Platform (MDP)** — платформе по детонации ВПО. Платформа позволяет открыть подозрительный файл без ущерба инфраструктуре в специализированной виртуальной среде для дальнейшего изучения и анализа. Платформа MDP проводит глубокий поведенческий анализ следующих объектов:

- Файлов и архивов в явном виде — при формировании запроса на анализ возможно прикреплять как файлы различных форматов, так и архивов, в том числе защищенных паролем (пароль задается в соответствующем поле или подбирается из словаря системы);
- Объектов, доступных по ссылке — при формировании запроса на анализ возможно указывать ссылку в сети Интернет: система переходит по ссылке и подгружает полезную нагрузку для дальнейшего поведенческого анализа.

На главной странице представлен список со следующей информацией:

- Добавлено — дата и время отправки файла на проверку в MDP;
- Репортер — автор запроса на анализ файла в MDP;
- Файл — название файла, его SHA1 хэш и тип;
- Трояны — обнаруженное в файле вредоносного ПО в файле;
- Вердикт — вердикт о вредоносности файла. Под вердиктом отображается время, затраченное на проверку файла;
- Отчет полигон — раскрывает в новой вкладке страницу с подробным отчетом о проверке файла.

Если файл получил вердикт «Вредоносный», рядом с названием файла появится размер файла и значок загрузки, с помощью которого можно скачать файл с ВПО.

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

- Мои загрузки — будут показаны отчеты о файлах, отправленных Пользователем;
- Вредоносный — будут показаны отчеты только о файлах с вердиктом «Вредоносный»;
- Статус — данные по статусу проверки файла;
- Вердикт — данные по одному или нескольким вердиктам;
- Тип — фильтрация по типу проверенного файла;
- Компания — данные по одной или нескольким компаниям;
- Репортер — данные по одному или нескольким авторам запроса;
- Начало – Конец — данные за указанный период времени;
-  — все фильтры.

С помощью кнопки **Загрузить** можно отправить файл или ссылку на проверку в систему MDP. Откроется всплывающее окно с формой для отправки.

Файл можно перетащить в специальное поле для загрузки или добавить с помощью кнопки «Найдите», либо добавить ссылку на файл в соответствующее поле. Лимит размера одного файла — 100 МБ.

В форме можно настроить параметры анализа файла, такие как:

- Параметры запуска — период и приоритет запуска;
- Системная конфигурация — настройки для конфигурации опций MDP;
- Виртуальные машины — выбор одной или нескольких виртуальных машин для генерации отчета;
- Параметры анализа: эмуляция пользовательской активности, настройки сети, статистический анализ.

3.3.3 Конфигурации

Во вкладке **Конфигурации** представлена информация о вариантах реализации вредоносных программ, нацеленных на инфраструктуру Заказчика. Сбор информации формируется при исследовании большого множества вредоносных файлов и расследовании различных инцидентов.

Заказчик получает уведомление, если вредоносная программа имеет файл настроек, где затрагиваются его системы, IP-адреса, домены и внешние телефоны пользователей.

На главной странице представлен список со следующей информацией:

- Первое и последнее появление ВПО;
- Config hash — SHA1 хэш файла;
- Вредоносное ПО — название семейства ВПО.

При нажатии на строку открывается всплывающее окно с подробной информацией о вредоносном ПО.

Также информация во вкладке **Конфигурации** поделена на подразделы:

- **Все** — главная страница, список всех конфигураций;
- **Соответствует Hunting правилам** — данные, содержащие доменные имена компании Пользователя.

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

- Трояны — фильтрация по одному или нескольким семействам ВПО;
- Начало – Конец — данные за указанный период времени.

Также данные можно выгрузить в виде CSV-файла с помощью кнопки загрузки.

С помощью кнопки **Загрузить** можно отправить конфигурацию вредоносного ПО. При нажатии на кнопку откроется всплывающее окно с формой для отправки.

Файл можно перетащить в специальное поле для загрузки или добавить с помощью кнопки **Browse**.

В форме необходимо заполнить следующие поля:

- SHA1 — SHA1 хэш файла вредоносного ПО;
- Имя файла;
- Config extracted — дата обнаружения конфигурации ВПО;
- Трояны — выбор ВПО, связанного с описываемым.

3.3.4 Фишинг комплекты

Во вкладке **Фишинговые комплекты** представлена информация об архивах фишинговых комплектов.

Фишинг-комплект или фишинг-кит — это набор страниц, скриптов и изображений, обеспечивающих работу фишингового сайта. Другими словами, это готовый фишинговый сайт с соответствующим файлом настроек, в котором могут указываться параметры отображения страницы, инструкции о том, как поступать с полученными данными: сохранять локально, производить запись в базу данных или отправлять на указанный адрес электронной почты (самый распространенный вариант).

На главной странице представлен список со следующей информацией:

- Дата обнаружения ресурса;
- Фишинг комплект — хэш-сумма фишинг кита и ресурс, для которого он предназначается;
- Извлеченные электронные письма — перечисление преднастроенных почтовых адресов, на которые отправляются данные. Адреса извлекаются из конфигурационных файлов фишинг-комплекта автоматически.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы**.

При нажатии на строку открывается подробная информация о ресурсе.

Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию за указанный период времени.

С помощью кнопки  слева от поисковой строки можно отсортировать информацию с помощью фильтров:

- Параметры — можно выбрать скрытые или добавленные в избранное данные;
- Бренд — данные по интересующему бренду/компании.

3.3.5 Уязвимости

Во вкладке **Уязвимости** представлена информация по обнаруженным уязвимостям в программном обеспечении по версиям. Помимо общей информации, также представлены данные по имеющимся эксплойтам с возможностью посмотреть ссылки на PoC (Proof-of-Concept), дополнительную информацию, либо возможность скачать этот эксплойт. На главной странице представлен список со следующей информацией:

- Дата обнаружения уязвимости;
- ID — глобальный идентификатор уязвимости;
- Эксплойты — наличие и количество общедоступных эксплойтов по уязвимости;
- Описание.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы.**

При нажатии на строку открывается подробная информация об уязвимости.

Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию за указанный период времени.

С помощью кнопки  слева от поисковой строки можно отсортировать информацию с помощью фильтров:

- Параметры — можно выбрать скрытые или добавленные в избранное данные;
- Опасность — данные по метке «severity»;
- Вендор — данные по производителю ПО, в котором была найдена уязвимость;
- Продукт — данные по названию продукта, в котором была найдена уязвимость;
- Версия — данные по версии ПО с уязвимостью;
- Тип;
- Оценка по CVSS;
- Обобщенная оценка CVSS;
- Оценка воздействия эксплойта;
- Оценка эксплойта по CVSS;
- Обобщенная оценка эксплойта по CVSS;
- Есть эксплоит;
- Эксплуатируемость.

3.4 Атаки

Раздел **Атаки** содержит информацию о последних совершенных кибератаках и ресурсах, на которые были совершены эти атаки. Эти данные разделены по вкладкам:

- Фишинг;

- DDoS-атаки;
- Дефейсы.

3.4.1 Фишинг

Во вкладке **Фишинг** представлена информация о различных фишинговых ресурсах (в том числе на такие сайты как Google, Microsoft и т.п.) в сети Интернет. В данный подраздел попадает только подтвержденная информация по фишинговым ресурсам. На главной странице представлен список со следующей информацией:

- Дата обнаружения;
- Тип нарушения;
- Ссылка;
- Бренд — название бренда/компании, под который мимикрирует фишинговый ресурс.

При нажатии на строку открывается подробная информация о ресурсе.

Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию за указанный период времени.

Рядом с поисковой строкой расположены быстрые фильтры, с помощью которых можно отсортировать информацию:

- Выбор группировки данных — позволяет сгруппировать данные по домену, по хостингу, по регистратору;
- Бренд — данные по интересующему бренду/компании;
- Дата обнаружения — данные за выбранный период времени.

С помощью кнопки  можно открыть дополнительные фильтры:

- Диапазон дат — фильтрация по дате обнаружения;
- Тип нарушения — фильтрация по типу нарушения;
- Источники — фильтрация по одному или нескольким источникам;
- Обогащение — обогащенные или необогащенные данные.

Необходимые данные можно выбрать с помощью чекбокса и выгрузить в виде CSV-файла с помощью кнопки загрузки  .

С помощью кнопки **Сканировать URL** Пользователь может сканировать URL-адрес, чтобы установить, является ли он фишинговым или легитимным.

3.4.2 DDoS-атаки

Во вкладке **DDoS-атаки** представлена информация о ресурсах в сети Интернет, которые подвергаются DDoS-атакам различного типа. Данные пополняются и обновляются

в режиме реального времени. На главной странице представлен список со следующей информацией:

- Первое появление — дата и время обнаружения атаки;
- Домен жертвы;
- IP жертвы;
- Страна жертвы;
- Тип DDoS-атаки.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы**.

При нажатии на строку открывается всплывающее окно с подробной информацией об атаке.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, в которых упоминаются доменные имена или ключевые слова, относящиеся к компании Пользователя;
- Тип DDoS атаки — фильтрация по типу атаки;
- Страна жертвы — фильтрация по одной или нескольким странам;
- Начало – Конец — данные за указанный период времени;
-  - все фильтры.

Также данные можно выгрузить в виде CSV-файла с помощью кнопки загрузки  .

3.4.3 Дефейсы

Во вкладке **Дефейсы** представлена информация о ресурсах в сети Интернет, на которых произошел дефейс сайта (подмена, искажение визуального содержимого веб-сайта). Чаще всего его производят веб-хулиганы (форма вандализма) или хактивисты (политическая или религиозно мотивированная группировка злоумышленников) с целью привлечения внимания. После успешной атаки они публикуют эту информацию на специализированных сайтах, посвященных дефейсам, в социальных сетях или на персональных сайтах. На главной странице представлен список со следующей информацией:

- Обнаружено — дата обнаружения дефейса;
- Цель — домен или IP-адрес ресурса, который подвергается атаке, и страна нахождения;
- Преступная группа.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы**.

При нажатии на строку открывается подробная информация об атаке.

Во вкладке можно найти необходимую информацию с помощью поисковой строки, а также отсортировать информацию за указанный период времени. С помощью кнопки  слева от поисковой строки можно отсортировать информацию с помощью фильтров:

- Источник — фильтрация по одному или нескольких источникам;
- Главная страница — будут показаны данные об атаке, произведенной на главную страницу ресурса;
- Преступная группа — данные по одной или нескольким группам злоумышленников;
- Страна — данные по одной или нескольким странам.

3.5 Опасные IP

Раздел **Опасные IP** содержит информацию об IP-адресах, которые используют злоумышленники. Эти данные разделены по вкладкам:

- Tor;
- Открытые прокси;
- Socks прокси на боте;
- Сканирование IP;
- VPN.

3.5.1 Tor

Во вкладке **Tor** представлена информация о выходных серверах сети TOR. Последние в цепочке серверы TOR называются выходными узлами. Они выполняют роль передаточного звена между клиентом сети TOR и публичным Интернетом. Многие злоумышленники используют выходные узлы TOR для совершения мошеннических действий.

На главной странице представлен список со следующей информацией:

- Первое и последнее появление — дата и время обнаружения выходного узла TOR и последней активности;
- Адреса Dir и OR — директории TOR или IP-адреса (v4 и v6) TOR серверов;
- Пропускная способность и флаги — пропускная способность TOR сервера и флаги, характеризующие данный TOR сервер;
- Владелец — владелец TOR сервера, указывается провайдер и почтовый ящик.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы**.

При нажатии на строку открывается всплывающее окно с дополнительной информацией.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, которые содержат IP-адреса, относящиеся к компании Пользователя;
- Начало – Конец — данные за указанный период времени.

Также данные можно выгрузить в виде CSV-файла с помощью кнопки загрузки.

3.5.2 Открытые прокси

Во вкладке **Открытые прокси** представлена информация о списках открытых прокси-серверов, публично распространяющихся на различных ресурсах, посвященных анонимности в сети. Все прокси-сервера в данном разделе были получены из открытых источников. На главной странице представлен список со следующей информацией:

- Первое и последнее появление — дата и время обнаружения открытого прокси-сервера и последней активности;
- Хост — IP-адрес открытого прокси и страна нахождения;
- Тип — наименование протокола;
- Источник — наименование/веб-адрес источника, откуда была получена информация о конкретном открытом прокси.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы**.

При нажатии на строку открывается всплывающее окно с дополнительной информацией.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, которые содержат IP-адреса, относящиеся к компании Пользователя;
- Страна — данные по одной или нескольким странам;
- Тип — данные по типу соединения;
- Источник — фильтрация по одному или нескольких источникам;
- Начало – Конец — данные за указанный период времени.

Также данные можно выгрузить в виде CSV-файла с помощью кнопки загрузки.

3.5.3 Socks прокси на боте

Во вкладке **Socks прокси на боте** представлена информация об адресах, где была установлена вредоносная программа, которая превращает компьютер в Socks-прокси. Такие компьютеры (боты) сдаются в аренду и используются при различных атаках, обеспечивая максимальный уровень анонимности атакующего. На главной странице представлен список со следующей информацией:

- Первое и последнее появление — дата и время обнаружения Socks прокси-сервера и последней активности;
- Хост — IP-адрес открытого прокси и страна нахождения;
- Источник — источник сбора данных, откуда была получена информация об определенном IP-адресе.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы**.

При нажатии на строку открывается всплывающее окно с дополнительной информацией.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, которые содержат IP-адреса, относящиеся к компании Пользователя;
- Страна — данные по одной или нескольким странам;
- Источник — фильтрация по одному или нескольких источникам;
- Начало – Конец — данные за указанный период времени.

Также данные можно выгрузить в виде CSV-файла с помощью кнопки загрузки.

3.5.4 Сканирование IP

Во вкладке **Сканирование IP** представлена информация о публичных и частных IP-адресах, которые были обнаружены в рамках мониторинга активности на honeypot-серверах. Honeypot-сервера — это хосты, которые умышленно выглядят уязвимыми для привлечения внимания злоумышленника. На главной странице представлен список со следующей информацией:

- Первое и последнее появление — дата и время обнаружения IP-адреса и последней активности с него;
- IP — обнаруженный IP-адрес;
- Теги;
- Источник — источник сбора данных, откуда была получена информация об определенном IP-адресе.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы**.

При нажатии на строку открывается всплывающее окно с дополнительной информацией.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, которые содержат IP-адреса, относящиеся к компании Пользователя;
- Теги — данные по одному или нескольким тегам;
- Источник — фильтрация по одному или нескольких источникам;
- Начало – Конец — данные за указанный период времени.

Также данные можно выгрузить в виде CSV-файла с помощью кнопки загрузки  .

3.5.5 VPN

Во вкладке **VPN** представлена информация по IP-адресам публичных и приватных VPN серверов, которые могут быть использованы злоумышленниками для сокрытия своих вредоносных действий. На главной странице представлен список со следующей информацией:

- Первое и последнее появление — дата и время обнаружения IP-адреса и последней активности с него;
- Хост — IP-адрес открытого прокси и страна нахождения;
- Тип — один из трех типов VPN сервисов (см. ниже) к которому относится данный IP;
- VPN name — название VPN сервиса, которому принадлежит данный IP-адрес;
- Наименование сигнатуры — внутреннее название правила реагирования.

Типы VPN сервисов:

Тип сервиса	Описание
Self-hosted	Созданный лично VPN сервер, который настраивается на личном оборудовании автора, либо на арендованном облачном сервере. Самые опасные, чаще всего используются высококвалифицированными злоумышленниками. Блокировать все self-hosted VPN без разбора нельзя - может встретиться легитимный self-hosted VPN, который был поднят не с целью нанесения вреда.

Тип сервиса	Описание
Public	Публичный открытый VPN сервер. (к примеру - Windscribe, OpenVPN и т. д.) Любой человек может купить этот VPN, либо использовать его бесплатно. Недоверенный источник. Злоумышленники редко используют для своих целей.
Commercial	Коммерческие VPN сервера. Официальные VPN-решения от различных вендоров. Обычно используются большими компаниями. Как правило, не используются злоумышленниками активно, но могут использоваться в случае компрометации коммерческого VPN-сервера.

Каждая строка также отмечена меткой «severity», которая обозначается цветовым индикатором в левой части карты. Подробнее про метку описано в пункте **3.2.4 Открытые угрозы**.

При нажатии на строку открывается всплывающее окно с дополнительной информацией.

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

- Правила для Threat Hunting — фильтр отображает релевантные данные, для которых специалистами Разработчика созданы автоматические правила детектирования сетевой инфраструктуры или новых атак;
- Страна — данные по одной или нескольким странам;
- VPN name — фильтрация по названию VPN сервиса;
- Начало – Конец — данные за указанный период времени;
-  — все фильтры.

Также данные можно выгрузить в виде CSV-файла с помощью кнопки загрузки  .

3.6 Граф

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

У Пользователя существует возможность ввести один из параметров (IP-адрес, домен, SSL и SSH-сертификат, Email, номер телефона, никнейм, хэш) интересующего его объекта и получить по нему дополнительный контекст в виде графа с узлами связи. Кроме того, граф можно построить на основе данных за указанный период.

Инструментарий раздела позволяет автоматически производить построение графа связности исследуемого ресурса или узла с другими типами объектов:

- **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;
- **Emails** — почтовые адреса, используемые при регистрации доменов;
- **Телефоны** — телефонные номера, используемые при регистрации доменов;
- **Кибер-криминальные группировки** — группировки злоумышленников, связанные с исследуемым хостом или доменом;
- **Семейство вредоносного ПО** — семейство ВПО, связанное с исследуемым хостом или доменом;
- **Профили** — профили злоумышленников в социальных сетях, связанные с обнаруженными контактными данными с именами пользователей.

Узлы графа имеют различные цвета в зависимости от их значения:

Цвет	Значение	Описание
Синий	Социальные сети	Ресурсы социальных сетей и мессенджеров
Зеленый	Сеть	Сущности, связанные с сетью Интернет
Красный	Вредоносная активность	Все сущности, связанные с вредоносным ПО
Оранжевый	Хакерская активность	Профили на специализированных форумах
Желтый	Контактная информация	Перечисление контактных данных

Данные графа можно отобразить за определенный период времени, используя шкалу внизу интерфейса. Помимо этого, функциональными кнопками в правой панели возможно:

- Зафиксировать положение узлов графа (без движения);
- Отобразить хосты на карте мира;
- Сделать скриншот построенного графа;
- Отобразить граф в трехмерном виде;
- Отобразить граф во весь экран.