Руководство пользователя

Positive Technologies

ptsecurity.com

Дата редакции документа: 06.10.2025

Содержание

1. Об этом документе 4
2. О PT Fusion 5
3. Аппаратные и программные требования 6
4. Начало работы с PT Fusion 7
5. Обзор интерфейса PT Fusion 8
6. Раздел «Исследование угроз» 9
7. Раздел «Библиотека угроз» 25
8. Личный кабинет 31
9. Обновление и модернизация PT Fusion 32
10. Решение проблем 33
11. Обращение в службу технической поддержки 34
12. Гарантийное обслуживание 35

1. Об этом документе

Руководство пользователя содержит пошаговые инструкции и справочную информацию об использовании PT Fusion. В руководстве описаны ключевые и дополнительные функции PT Fusion, а также настройка функций для выполнения конкретных задач. Руководство не содержит инструкции по установке, первоначальной настройке и администрированию PT Fusion.

Руководство адресовано специалистам, использующим PT Fusion в своей работе.

2. О PT Fusion

PT Fusion (далее также — сервис) — это аналитический портал для получения актуальных данных о киберугрозах, в основу которого заложен опыт и лучшие практики команды PT ESC, полученные при исследованиях угроз, а также при расследованиях инцидентов информационной безопасности.

Краткое описание возможностей

Сервис позволяет решить следующие задачи:

- Загрузка и статический анализ файлов при помощи PT AV и YARA-правил PT ESC;
- Поведенческий анализ загруженных файлов в безопасной среде (Sandbox) с отображением имен поведенческих, сетевых вердиктов PT ESC, а также тактик и техник, которые использует файл в процессе работы согласно матрице MITRE ATT&CK;
- Получение извлеченной метаинформации по 28 типам файлов;
- Поиск похожих файлов по аналогичной метаинформации;
- Поиск информации по индикаторам компрометации: хеш-суммам, IP-адресам, URL, доменам;
- Классификация и атрибуция ВПО, а также связанных с ним индикаторов компрометации;
- Отображение связей с вредоносными файлами, сетевыми индикаторами, группировками и семействами ВПО;
- Поиск информации о сетевых ресурсах в PT PDNS;
- API-доступ и автоматизация запросов к порталу;
- Поиск информации об APT-группировках, целях и используемых ими техниках, тактиках и процедурах (TTP) в соответствии с MITRE ATT&CK с целью построения ландшафта угроз (название, описание, когда встречались, альтернативные названия, цели, какие отрасли страны атакуют, связанные публичные отчеты, уязвимости, инструменты).

Уровень подготовки пользователей

Все пользователи сервиса должны иметь навыки работы с браузерами.

3. Аппаратные и программные требования

Чтобы подключиться к сервису и получить доступ к его ресурсам, необходимо АРМ с установленным на него браузером Google Chrome 84+ (или другим на основе Google Chrome 84+).

4. Начало работы с PT Fusion

Для работы в сервисе необходимо приобрести подписку. После этого сервисный менеджер должен создать учетную запись пользователя и прислать вам логин и пароль для входа.

► Чтобы авторизоваться в сервисе:

1. В адресной строке браузера введите fusion.ptsecurity.com.
2. Откроется страница входа в PT Fusion.
3. Введите имя пользователя и пароль.
4. Нажмите **Войти.**

5. Обзор интерфейса PT Fusion

В верхней части страницы расположено главное меню. Оно содержит разделы для перехода к страницам сервиса:

- Переключение раздело между «Исследованием угроз» и «Библиотекой угроз»
- Поиск – раздел для поиска по индикаторам компрометации и загрузки файлов на анализ
- Иконка аккаунта – раздел, содержащий подразделы для смены пароля, изменению языка интерфейса и изменению темы портал

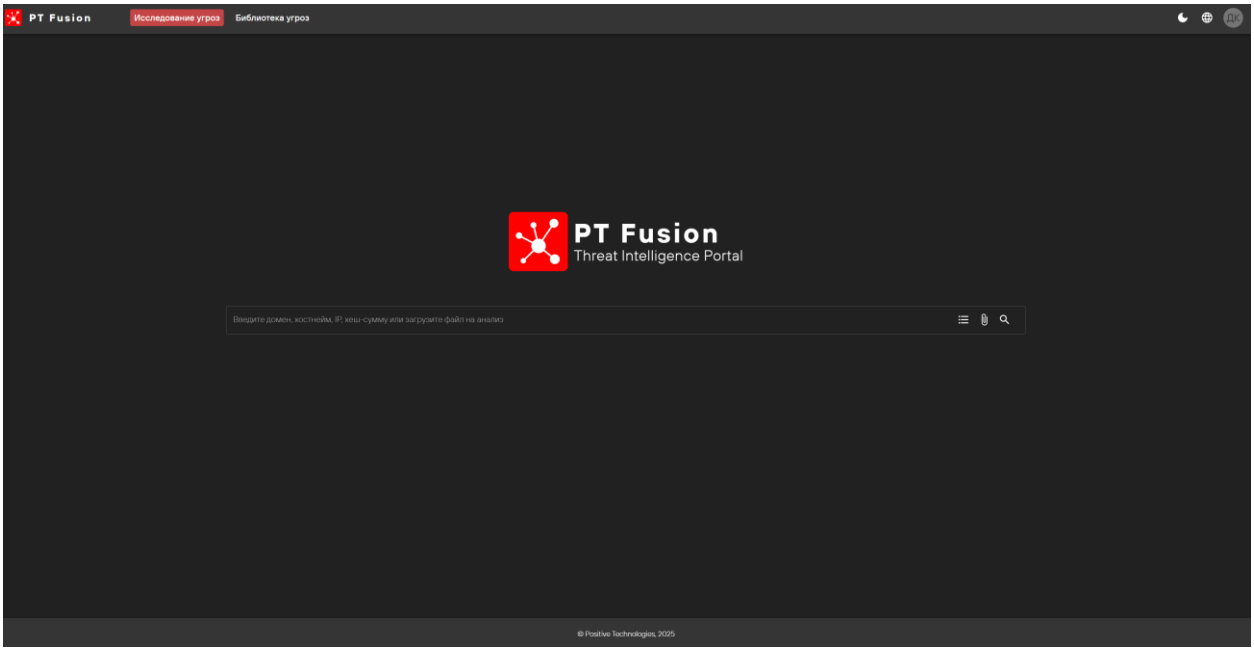

Рисунок 1. Главная страница PT Fusion

6. Раздел «Исследование угроз»

В разделе «Исследование угроз» пользователь может отправлять файлы на проверку, искать индикаторы компрометации и также осуществлять параметризованный поиск по различным полям, описанным ниже.

Загрузка файла на анализ

Для отправки файла на анализ необходимо нажать кнопку . После этого откроется диалоговое окно:

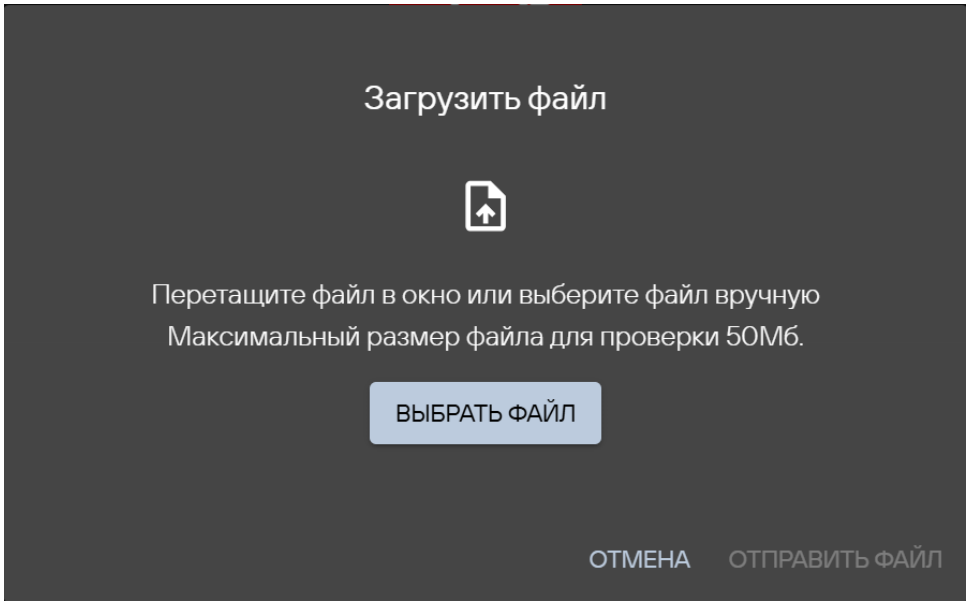

Рисунок 2. Окно загрузки файла

Для отправки файла можно перетащить файл из проводника ОС в это диалоговое окно и нажать кнопку «ОТПРАВИТЬ ФАЙЛ» или нажать кнопку «ВЫБРАТЬ ФАЙЛ», выбрать необходимый файл в проводнике ОС и затем нажать кнопку «ОТПРАВИТЬ ФАЙЛ».

После отправки файла необходимо дождаться полного анализа файла.

Поиск в разделе «Исследование угроз»

В портале реализован поиск двух типов – не параметризованный и параметризованный

Не параметризованный поиск

Не параметризованный поиск позволяет искать по основным индикатора компрометации:

- IPv4
- Доменам
- Хостнеймам
- DNS-записям
  - MX
  - NS
- Хеш-суммам:
  - MD5
  - SHA1
  - SHA256

Параметризованный поиск

Параметризованный поиск позволяет искать связанные индикаторы по:

- Общим полям для всех типов файлов:
  - Ssdeep – параметр «**ssdeep**»
- Полям WHOIS домена:
  - Email зарегистрировавшего домен – параметр «**whois_email**»
- Полям для типов файлов EXE и DLL:
  - Imphash – параметр «**impash**»
- Полям для типа файла LNK:
  - Имя компьютера, на котором был создан файл – параметр «**lnk_machine**»
  - Серийный номер диска компьютера, на котором был создан файл – параметр «**lnk_drive_serial_number**»
  - Путь до иконки, которая отображается в ОС – параметр «**lnk_icon_location**»
  - Путь до файла, который исполнится при открытии LNK – параметр «**lnk_local_base_path**»
  - Относительный путь до файла, который исполнится при открытии LNK – параметр «**lnk_relative_path**»
  - Полностью или часть исполняемой команды при открытии LNK – параметр «**lnk_command**»

Любой запрос в параметризированном поиске осуществляется без кавычек. Между параметром и значение ставится знак двоеточие.

Результаты не параметризованного поиска

Результаты поиска по IP

После того, как пользователь ввел в поисковую строку IP адрес в интерфейсе появится карточка следующего вида.

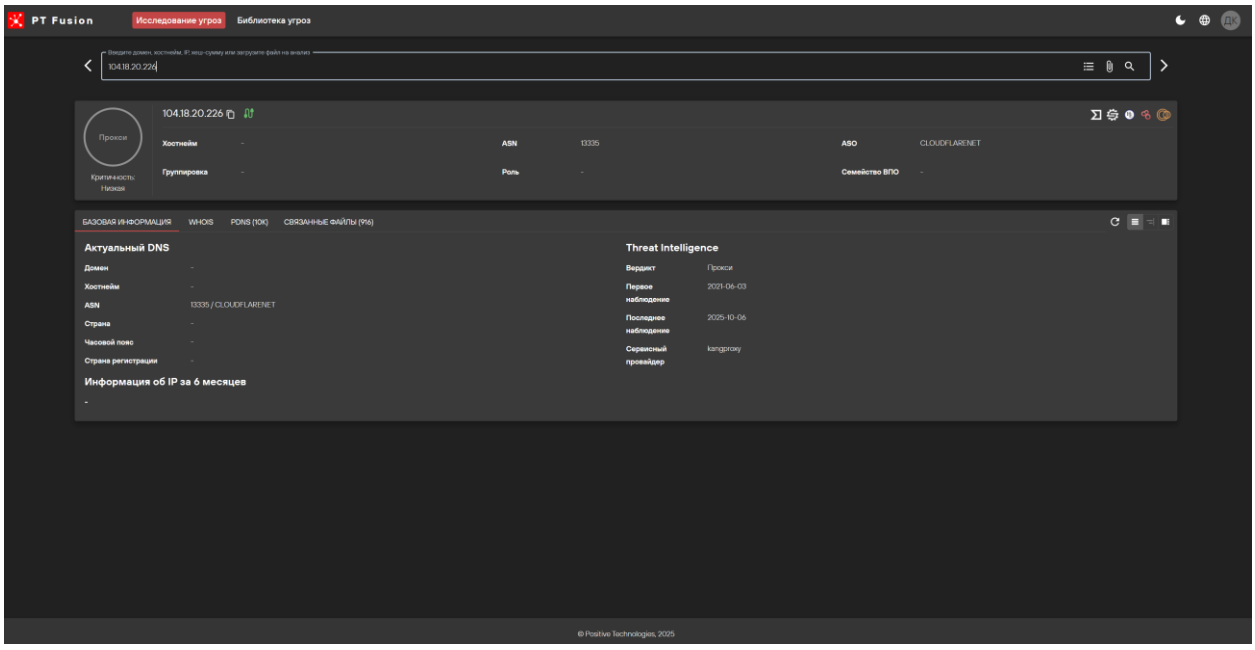

Рисунок 3. Карточка IP адреса

Карточка делится на два блока: верхний блок – это краткая информация об этом IP, нижний блок содержит детальную информацию в различных вкладках

Верхний блок

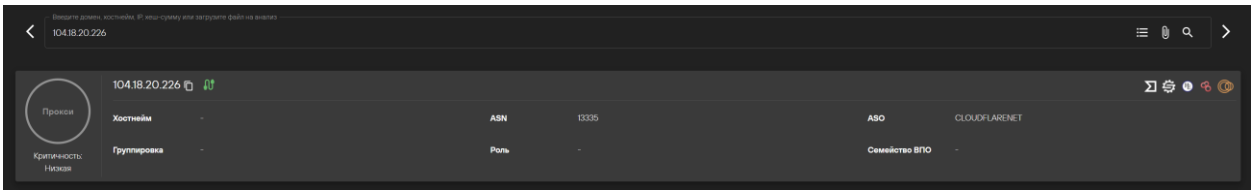

Рисунок 4. Верхняя карточка IP адреса

В верхней строке содержится информация об актуальном хостнейме, который сейчас расположен на IP, ASN к которой он принадлежит и название этого ASN.

В правом верхнем углу расположены ссылки на внешние ресурсы:

- https://www.virustotal.com/gui/ip-address/
- https://spur.us/context/
- https://bgp.he.net/ip/
- https://www.shodan.io/host/
- https://search.censys.io/hosts/

В нижней строке располагается информация об атрибуции этого IP к группировке, семейству ВПО, если он был замечен в атаках. Эти поля являются активными и, если пользователь нажмет на значение этого поля будет выполнен параметризованный запрос «**threat_actor:**» или же «**malware_family:**».

В левой части верхнего блока содержится вердикт для найденного IP.Ниже представлен список возможных вердиктов

Английская локализация	Русская локализация
Malicious	Вредоносный
Suspicious	Вероятно опасный
Clean	Чистый
Whitelisted	Безопасный
Unscored	Не определен
Scanner	Сетевой сканер
Tor node	TOR узел
Crawler	Сборщик данных
Sinkhole	Sinkhole
VPN gate	VPN шлюз
Proxy	Прокси
Cryptomining	Криптомайнинг

Torrent tracker	Торрент трекер
Parking	Запаркованный узел
Public dns server	Публичный DNS
Dyndns	DynDNS хостинг
Cloud	Облако
CDN	CDN узел
AD server	Рекламный сервер
Service	Интернет-сервис
IP to Domain	IP to Domain
Free email	Почтовый сервис
Crl ocsp	CRL/OCSP узел
Stun	STUN узел

Нижний блок

Нижний блок содержит детальную информацию об IP адресе. Для удобства информация разбита на по вкладкам.

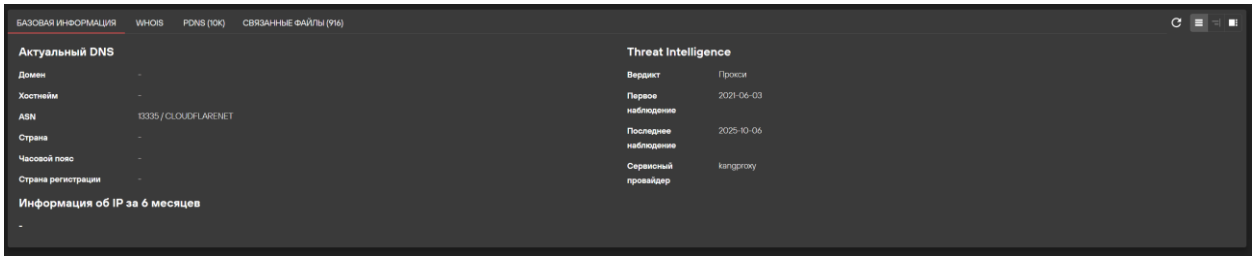

Рисунок 5. Нижний блок карточки IP адреса

Для IP в портале предусмотрено 4 вкладки.

Basic info / Базовая информация – расширенная информация из верхней карточки. Так же представлены данные из Threat intelligence. Для вердиктов Proxy и VPN будет отображено поле «Сервисный провайдер», указывающее на поставщика услуг. Для вредоносных индикаторов будут указаны временные рамки, в течении которых был замечен этот IP, как вредоносный.

WHOIS – WHOIS данные этого IP.

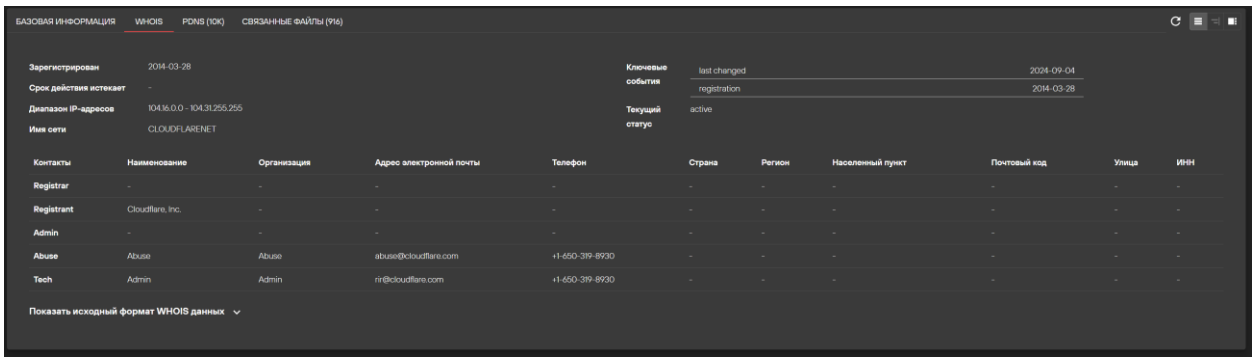

Рисунок 6. Карточка WHOIS IP адреса

PNDS – вкладка содержит историю резолвов доменов и хостнеймов. Значения в колонках Domain/Домен, Hostname/Хостнейм являются активными.

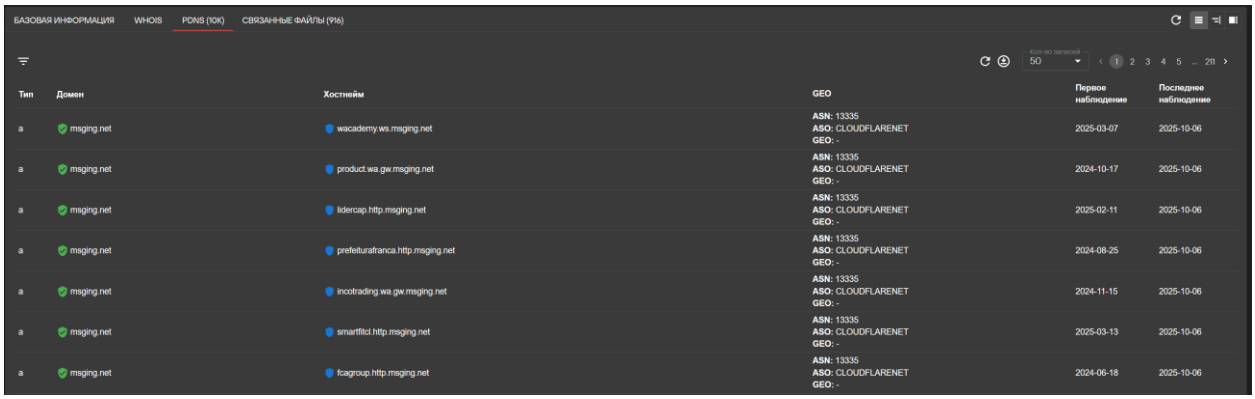

Рисунок 7. Карточка PDNS IP адреса

Во вкладке можно использовать фильтры (левый верхний угол блока) для фильтрации нужных доменов, хостнеймов или использовать фильтр по датам.

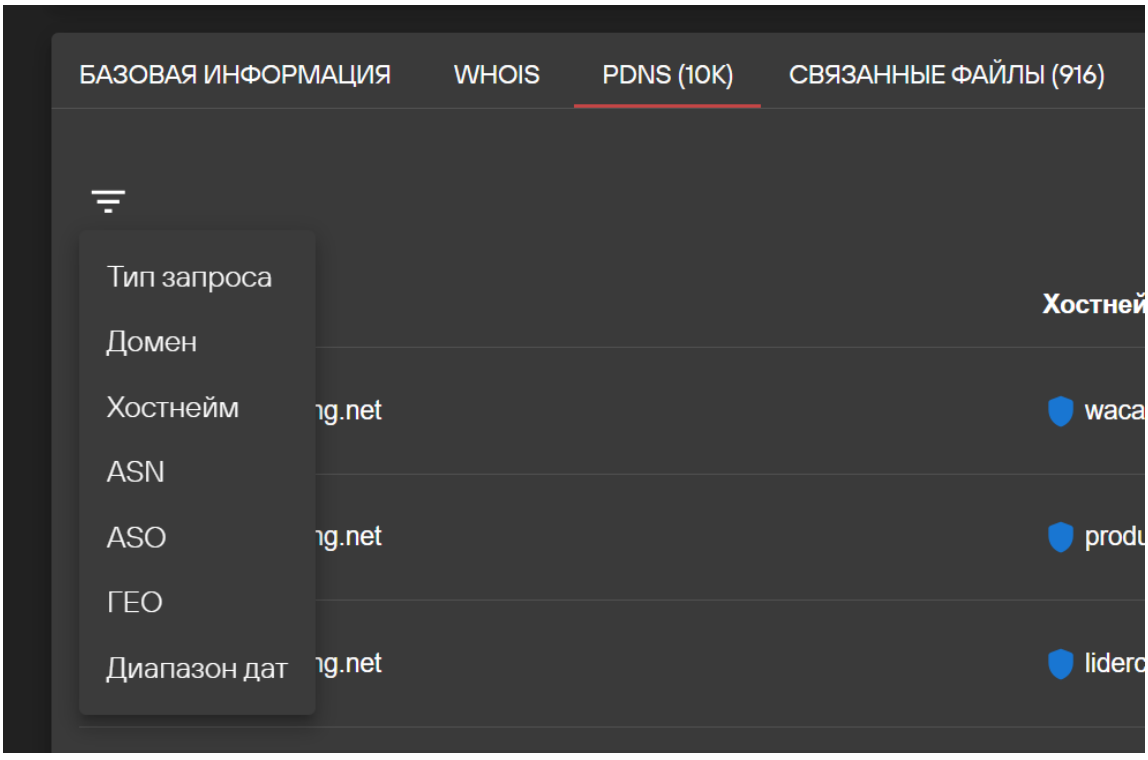

Рисунок 8. Окно выбора фильтра по результатам в PDNS для IP адреса

Левый угол блока содержит кнопки переключения табличного и графового представления, сводку по данным в таблице, а также предоставляет возможность скачать результаты PDNS таблицы в виде CSV.

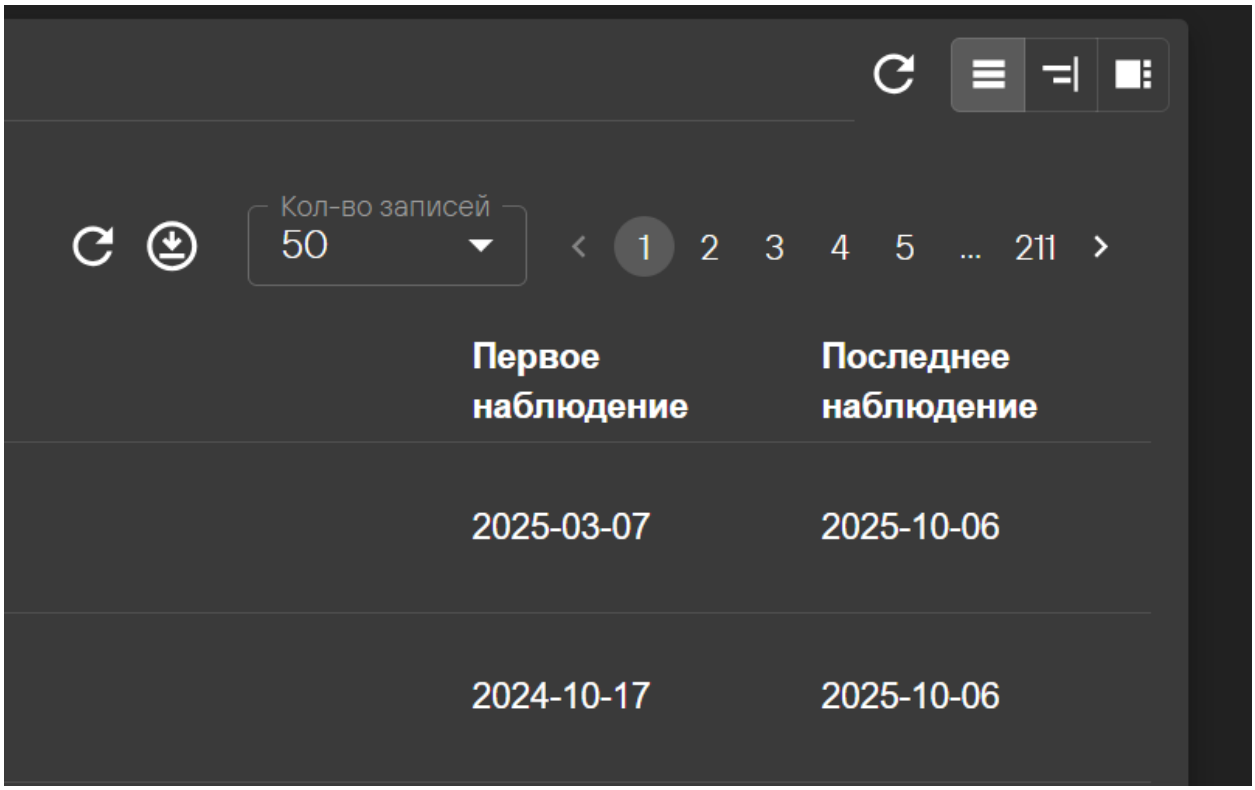

Рисунок 9. Кнопки переключения отображения представлений, отображение сводки и скачивания результата поиска в PDNS в CSV формате

Графовое представление позволяет удобнее работать с данными.

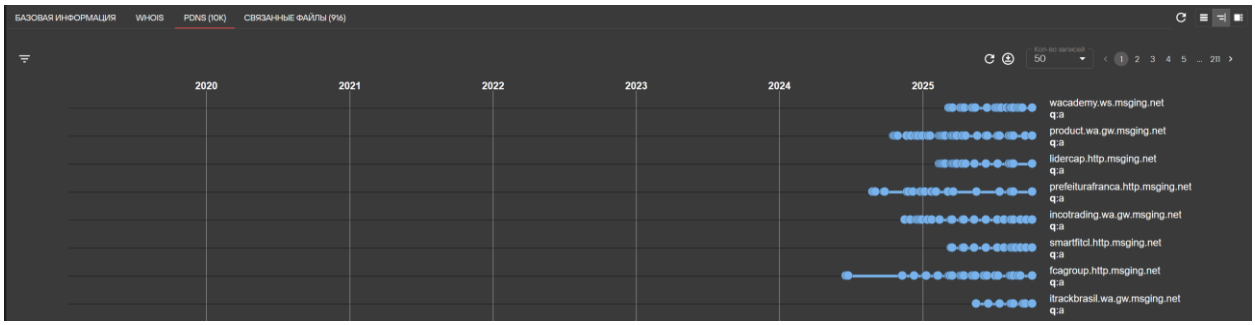

Рисунок 10. Графовое представление данных из PDNS IP адреса

Сводка показывает суммаризацию по представленным данным. Поля в сводке являются активными и позволяют по нажатию строить фильтры.

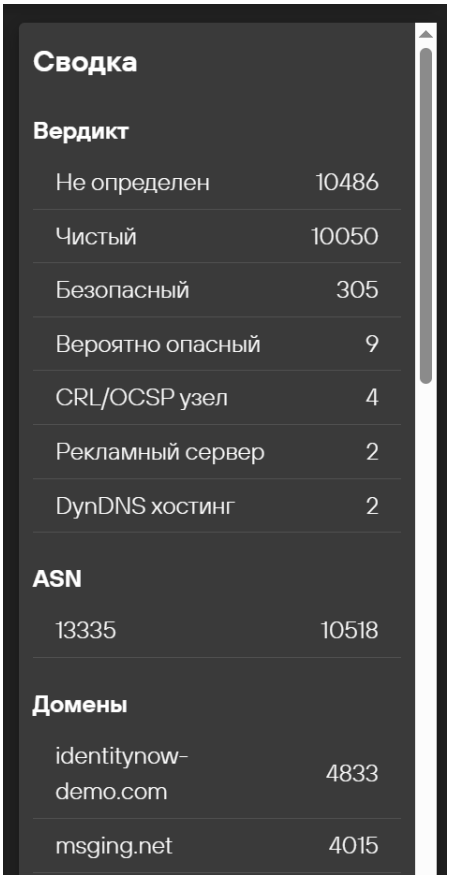

Рисунок 11. Отображение сводки таблицы PDNS IP адреса

Related files / Связанные файлы – на этой вкладке можно найти файлы, присутствующие в системе и которые соединяются с этим IP адресом или же этот этот IP присутствует в извлеченной конфигурации ВПО.

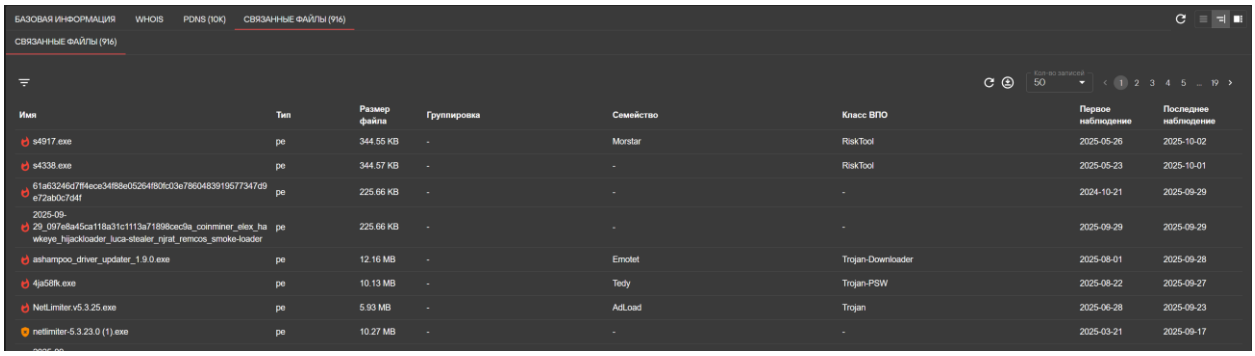

Рисунок 12. Вкладка со связанными файлами

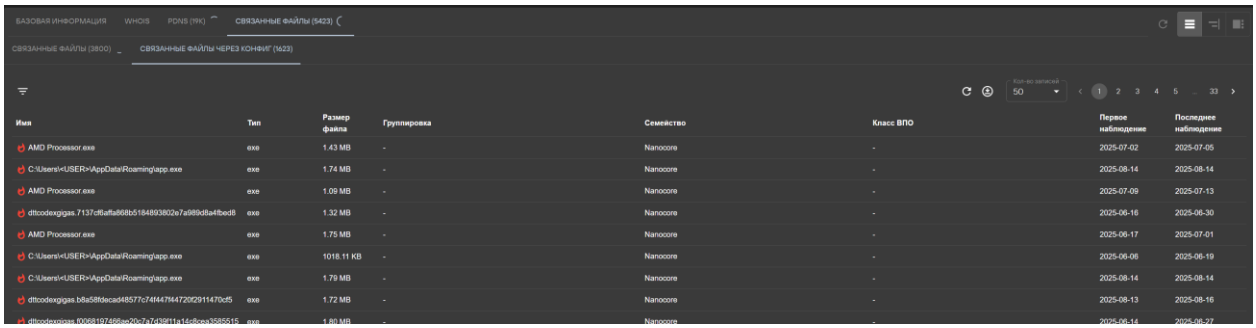

Рисунок 13. Вкладка со связанными файлами через извлеченную конфигурацию

Результат поиска по домену и хостнейму

После того, как пользователь ввел в поисковую строку домен в интерфейсе появится карточка следующего вида:

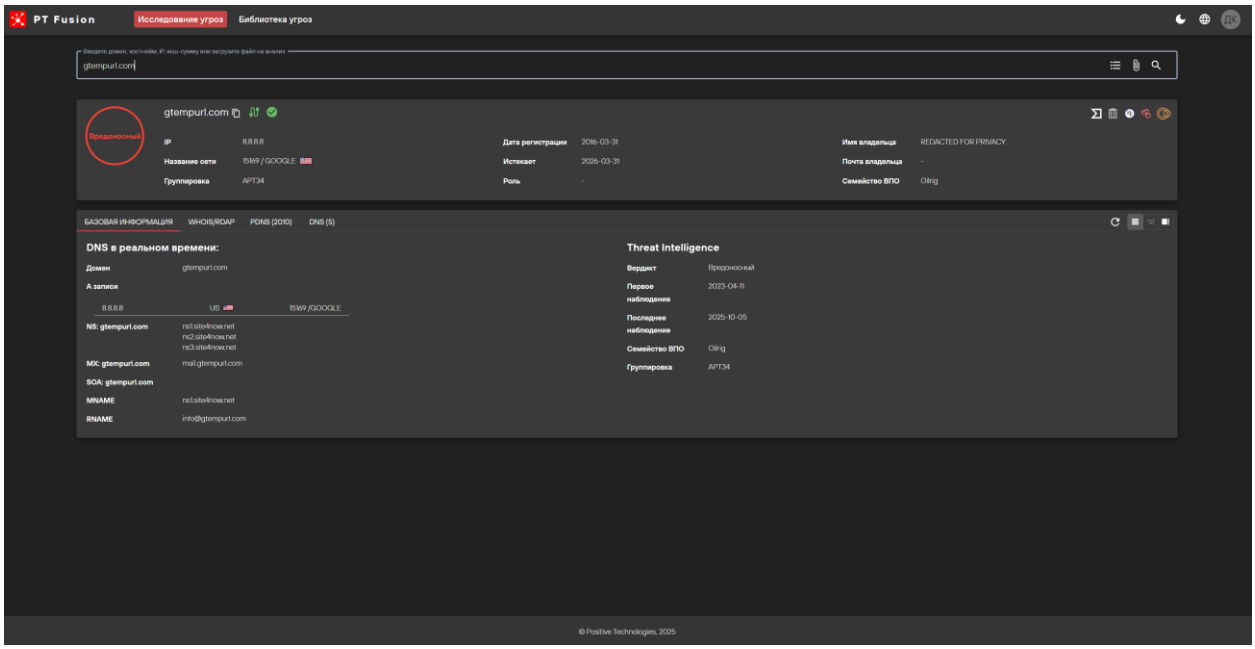

Рисунок 14. Карточка домена/хостнейма

Карточка делится на два блока: верхний блок – это краткая информация об этом домене/хостнейме, нижний блок содержит детальную информацию в различных вкладках.

Верхний блок

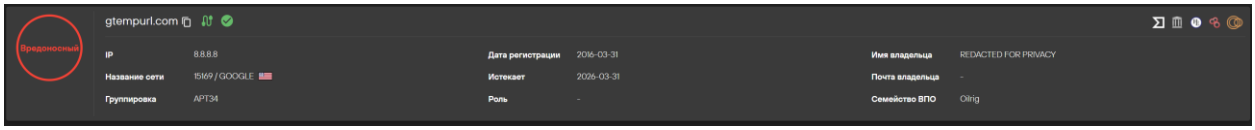

Рисунок 15. Верхний блок карточки домена/хостнейма

В левой части верхнего блока содержится вердикт для найденного домена. Ниже представлен список возможных вердиктов:

Английская локализация	Русская локализация
Malicious	Вредоносный
Suspicious	Вероятно опасный
Clean	Чистый
Whitelisted	Безопасный
Unscored	Не определен
Cryptomining	Криптомайнинг
Torrent tracker	Торрент трекер
Parking	Запаркованный узел

Public dns server	Публичный DNS
Dyndns	DynDNS хостинг
Service	Интернет-сервис
Crl ocsp	CRL/OCSP узел
Stun	STUN узел

В верхнем блоке содержится информация об актуальном резолве домена в IP

В правом верхнем углу расположены ссылки на внешние ресурсы:

- https://www.virustotal.com/gui/domain/
- https://web.archive.org/web/20250000000000*/
- https://bgp.he.net/dns/gtempurl.com#_dns
- https://www.shodan.io/search?query=
- https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=

В нижней строке располагается информация об атрибуции этого домена/хостнейма к группировке, семейству ВПО, если он был замечен в атаках. Эти поля являются активными и, если пользователь нажмет на значение этого поля будет выполнен параметризованный запрос «**threat_actor:**» или же «**malware_family:**».

Нижний блок

Нижний блок содержит детальную информацию о домене/хостнейме. Для удобства информация разбита на по вкладкам.

Basic info / Базовая информация – представляют собой расширенную информация из верхней карточки. Так же данные включают в себе актуальные DNS записи (NS, MX, SOA) домена/хостнейма. Так же представлены данные из Threat intelligence.

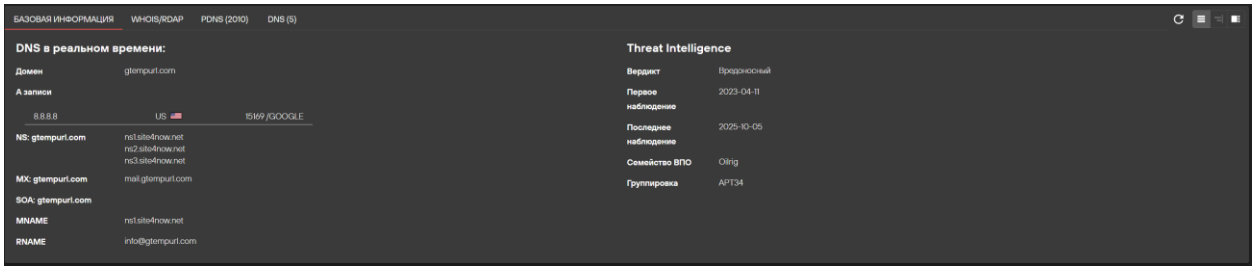

Рисунок 16. Нижний блок карточки домена/хостнейма. Базованя информация

WHOIS/RDAP – вкладка содержит актуальный, исторический WHOIS или RDAP домена. Разграничение выполнено в виде дополнительных вкладок.

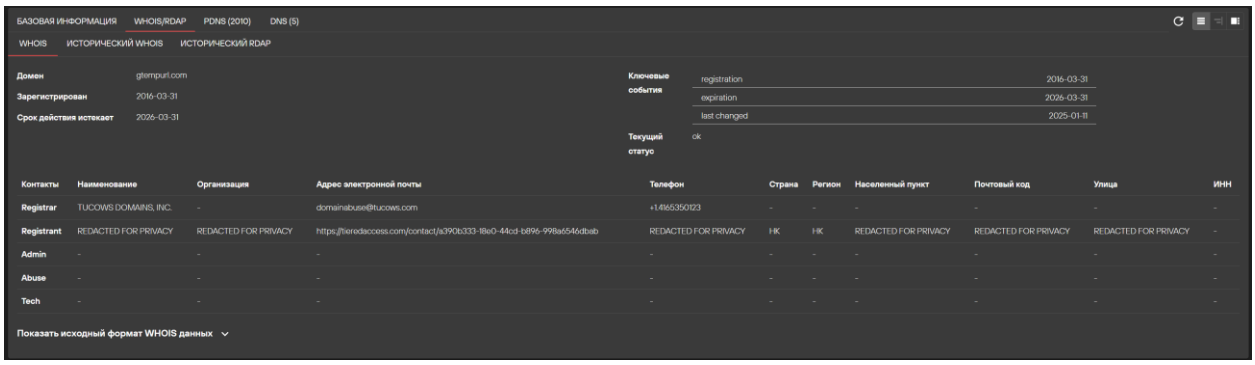

Рисунок 17. Нижний блок карточки домена/хостнейма. WHOIS/RDAP

PDNS – вкладка может быть выглядеть по разному в зависимости от того, что запросил пользователь – домен или хостнейм.

При запросе домена вкладка PDNS будет иметь две подвкладки – Домен/Domain и Хостнеймы/Hostnames. В первой подвкладке отображается PDNS для запрошенного домена. Во второй подвкладке будет отображен PDNS для поддоменов запрошенного домена.

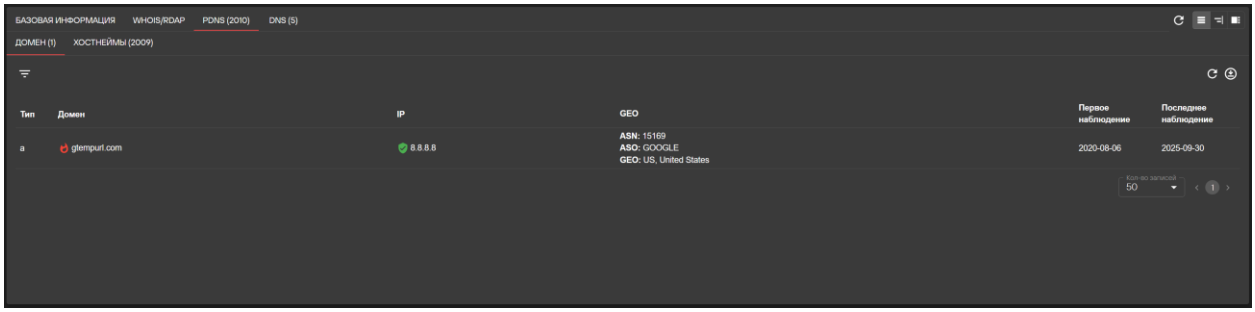

Рисунок 18. Нижний блок карточки домена/хостнейма. PDNS домена

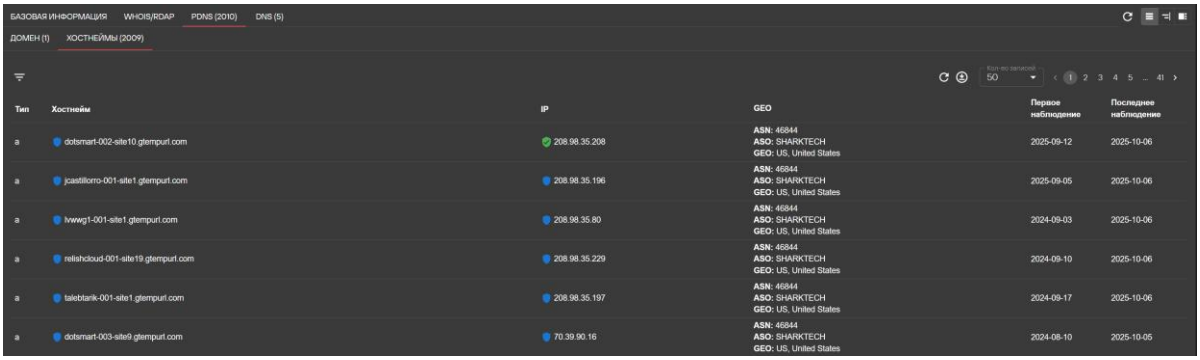

Рисунок 19. Нижний блок карточки домена/хостнейма. PDNS поддоменов

При запросе хостнейма вкладка PDNS будет будет отображен PDNS только запрошенного хостнейма.

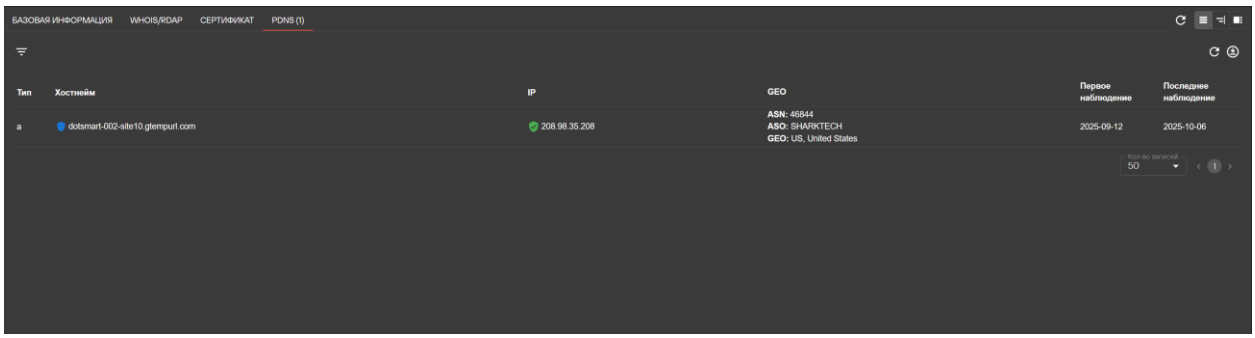

Рисунок 20. Нижний блок карточки домена/хостнейма. PDNS хостнейма

DNS – вкладка содержит информацию о NS, MX и SOA записях домена или хостнейма.

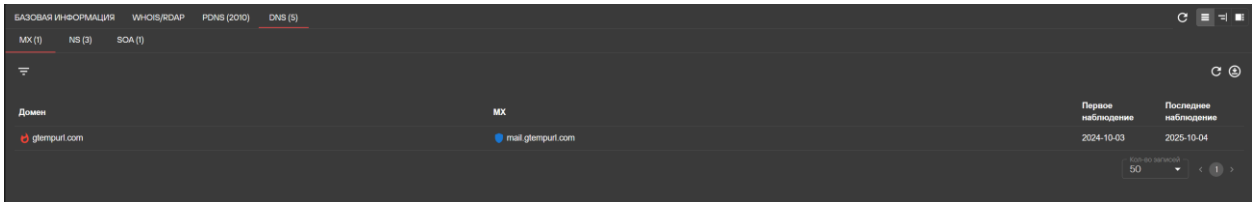

Рисунок 21. Нижний блок карточки домена/хостнейма. DNS записи домена/хостнейма

Related files / Связанные файлы – на этой вкладке можно найти файлы, присутствующие в системе и, которые соединяются с этим доменом/хостнеймом или же этот домен/хостнейм присутствует в извлеченной конфигурации ВПО.

Рисунок 22. Нижний блок карточки домена/хостнейма. Связанные файлы

Результат поиска по NS и MX серверам

В PT Fusion присутствует возможность поиска по NS и MX серверам. Поиск можно выполнить, как напрямую через поисковую строку, так и кликнув на соответствующую запись в разделе DNS, когда пользователь ищет домен или хостнейм.

При поиске по DNS записям будут показаны все домены, которые имеют соответствующую NS или MX записи в DNS.

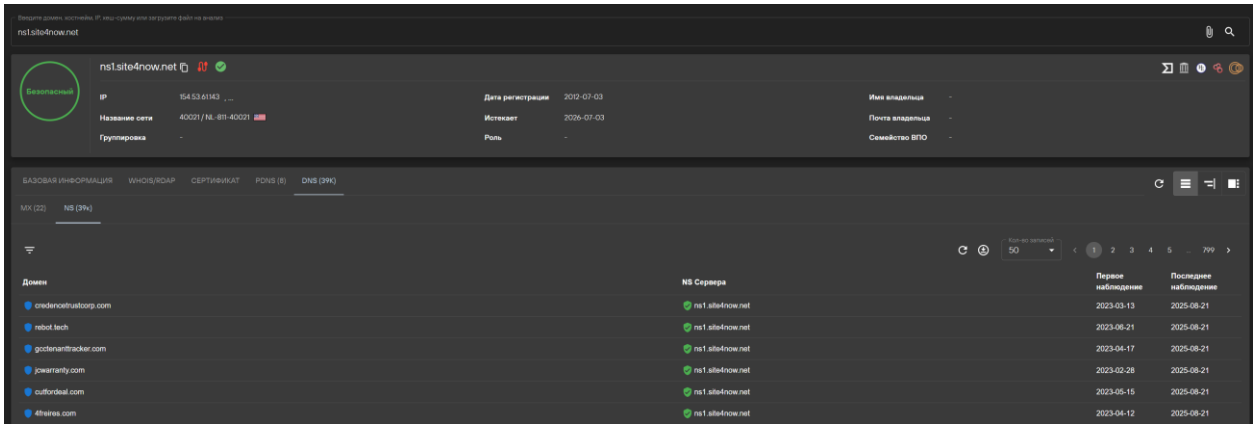

Рисунок 23. Пример поиска по NS Записи

Результаты поиска по хеш-суммам

После того, как пользователь ввел в поисковую строку хеш-сумму, в интерфейсе появится карточка следующего вида:

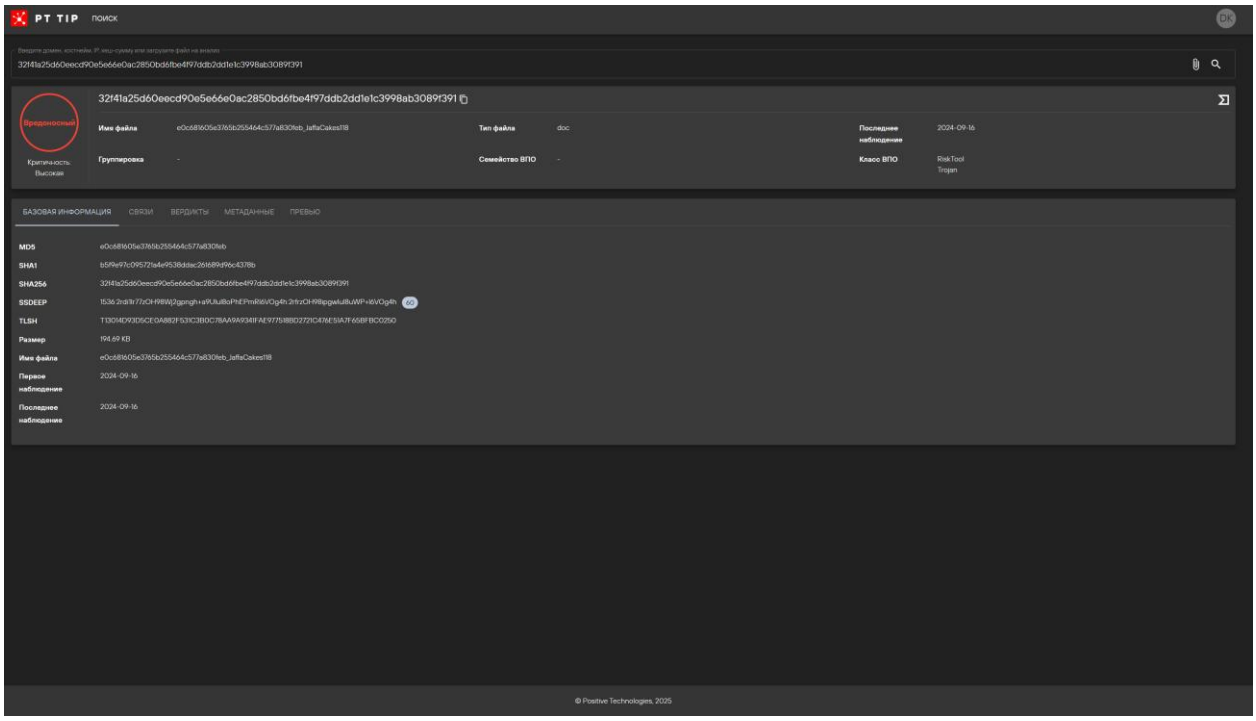

Рисунок 24. Результат поиска по хеш-сумме

Карточка делится на два блока: верхний блок – это краткая информация об этом файле, нижний блок содержит детальную информацию в различных вкладках.

Верхний блок

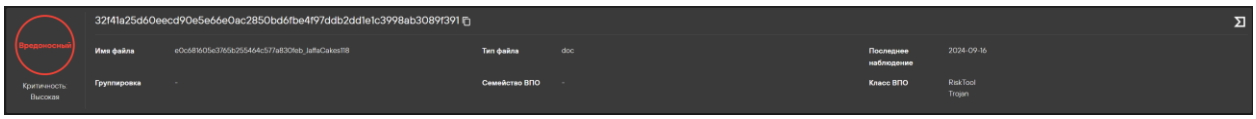

Рисунок 25. Верхний блок карточки хеш-суммы

В левой части верхнего блока содержится вердикт для файла, соответствующего запрошенной хеш-сумме. Ниже представлен список возможных вердиктов:

Английская локализация	Русская локализация
Malicious	Вредоносный
Suspicious	Вероятно опасный
Clean	Чистый
Whitelisted	Безопасный
Unscored	Не определен

В этом блоке так же можно найти информацию об имени файла, типе файла, о дате последнего наблюдения и информацию об атрибуции – какая группировка его использовала, к какому семейству и классу ВПО он принадлежит.

Нижний блок

Нижний блок содержит детальную информацию о файле. Для удобства информация разбита на по вкладкам.

Basic info / Базовая информация – содержит в себе основные хеш-суммы файла, имя файла, SSDEEP, TLSH, размер файла, имя файла и даты первого и последнего наблюдения.

Рисунок 26. Нижний блок карточки хеш-суммы

Relations / Связи – содержит информацию о связанных индикаторах, которые были получены в результате поведенческого анализа или были получены в результате статического извлечения.

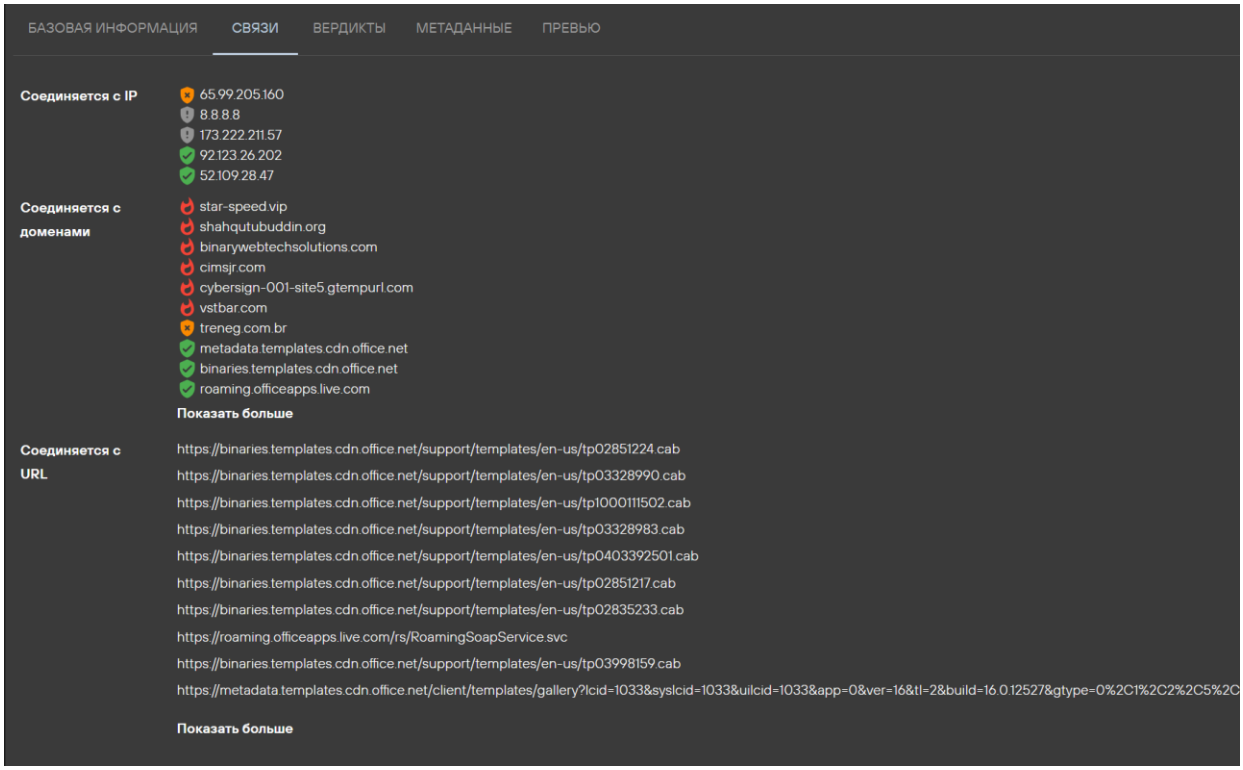

Рисунок 27. Связи файла с другими индикаторами

Verdicts / Вердикты – вкладка включает в себя информацию о детектах YARA-правил экспертного центра безопасности Positive Technologies (PT ESC), поведенческих и сетевых вердиктах PT Sandbox.

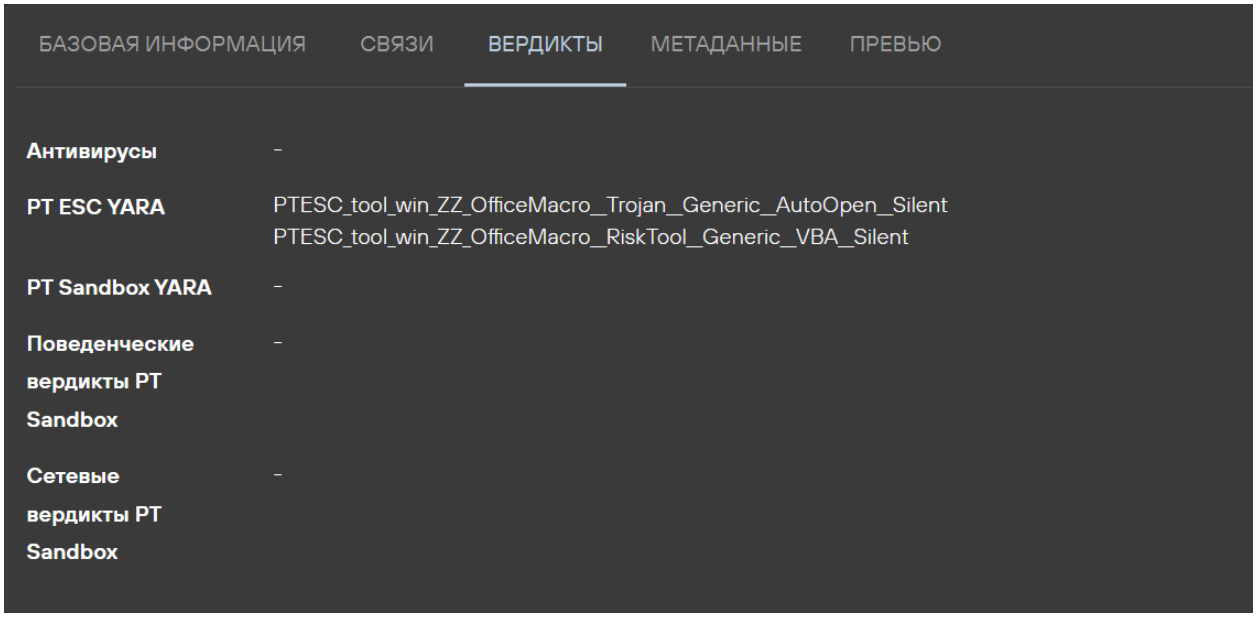

Рисунок 28. Вердикты на файл

Metadata / Метаданные - вкладка включает в себя информацию об извлеченных метаданных из файла. Для каждого типа файла набор метаданных будет свой.

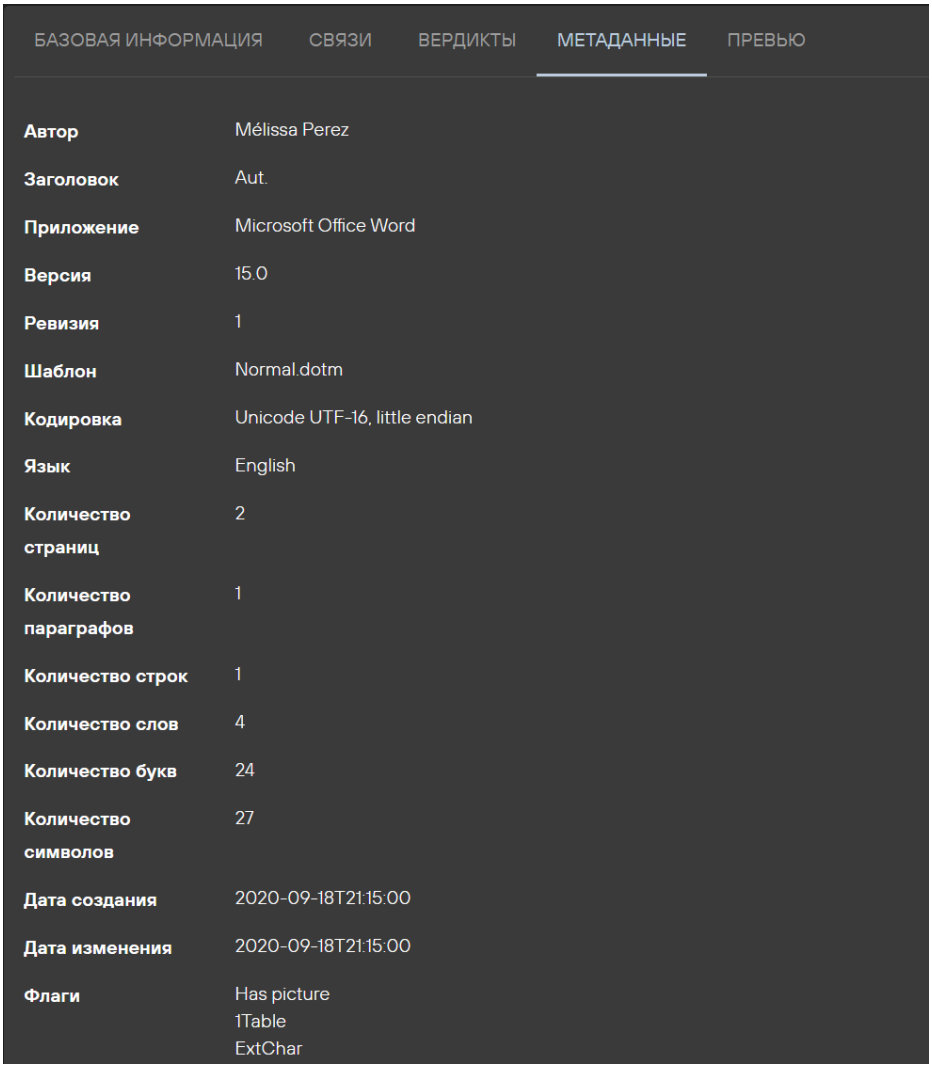

Рисунок 29. Метаданные файла

Preview / Превью – кнопка для отображения в интерфейсе скриншота первой страницы документа, письма или содержимого скриптовых файлов.

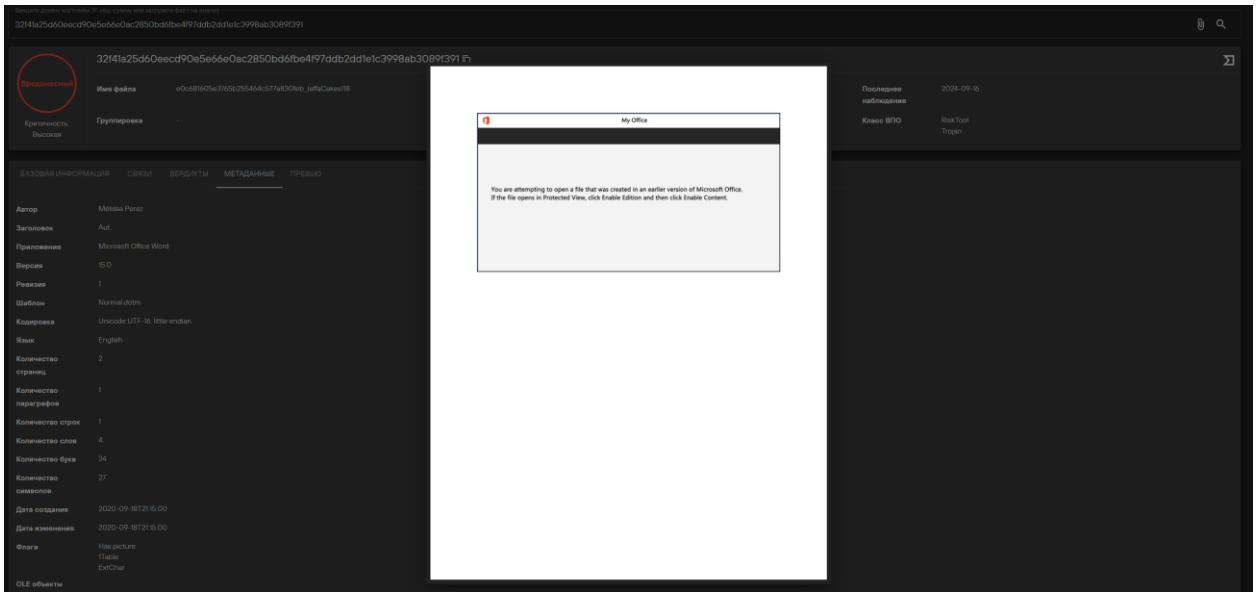

Рисунок 30. Превью файла

Результаты параметризованного поиска

Результаты поиска по SSDEEP

В портале поддерживается функции поиска индикаторов компрометации по SSDEEP файла. Искать по SSDEEP можно напрямую в поисковой строке с помощью параметра «**ssdeep:**» или в нижнем блоке карточки файла нажать на значение поля SSDEEP.

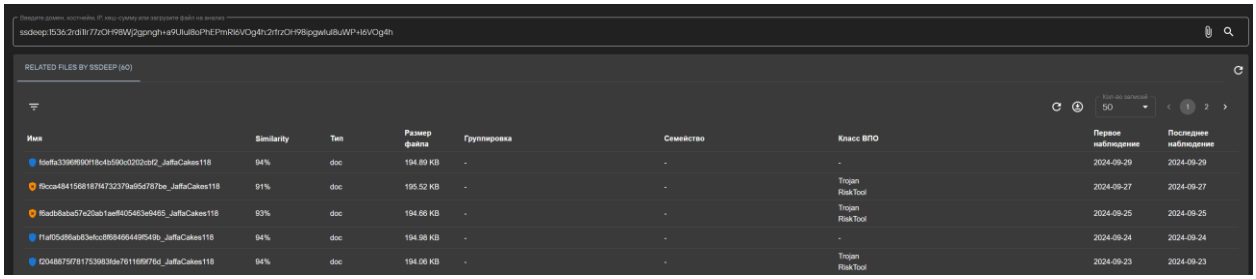

Рисунок 31. Результаты поиска по SSDEEP

В итоговой карточке отображены все файлы, которые имеют схожий с оригинальным SSDEEP. Также можно качать результаты поиска в CSV.

Результаты поиска по WHOIS

В портале поддерживается функции поиска индикаторов компрометации по почтовому ящику регистранта. Искать по этому этому ящику можно, как через поисковую строку с помощью параметра «**whois_email:**» или же нажав почтовый ящик регистранта в нижней карточке, во вкладке WHOIS/RDAP

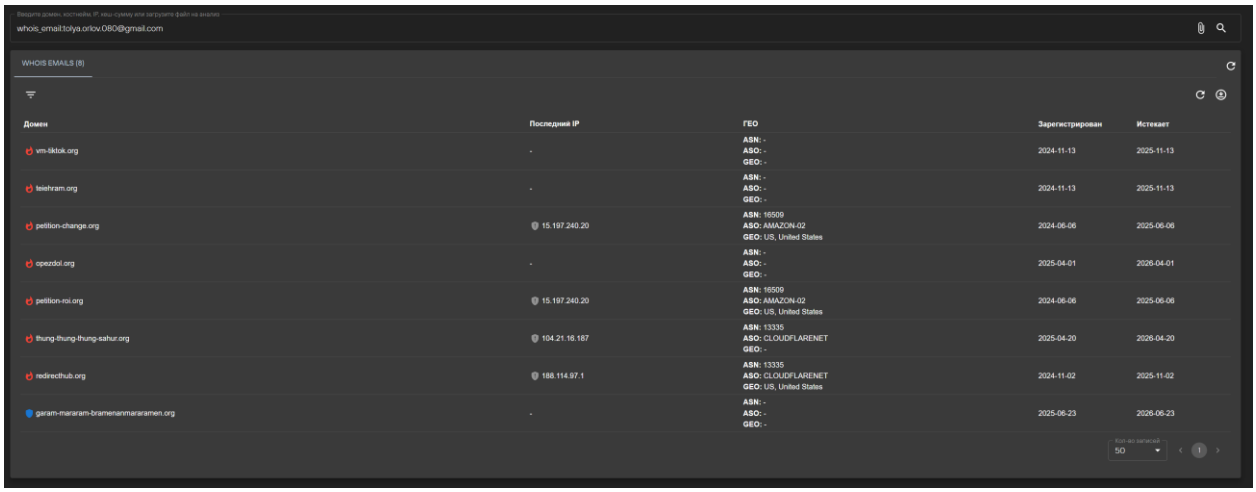

Рисунок 32. Результаты поиска по WHOIS

Результаты поиска по метаданным файлов

В портале поддерживается функции поиска индикаторов компрометации по различным метаданным файлов, описанных в п. 6.

Результат поиска по метаданным представляет собой таблицу, в которой собраны все файлы с таким же значением поля метаинформации по которому пользователь осуществлял поиск.

7. Раздел «Библиотека угроз»

Для того, чтобы перейти в раздел «Библиотека угроз» пользователю необходимо нажать на кнопку «Библиотека угроз» в верхней панели управления.

В разделе «Библиотека угроз» пользователь может получить информацию о группировках и их тактиках, техниках процедурах, связанных с группировками ВПО, утилитах, публичных отчетах, уязвимостях, а также полную информацию о каждой сущности и связях между ними.

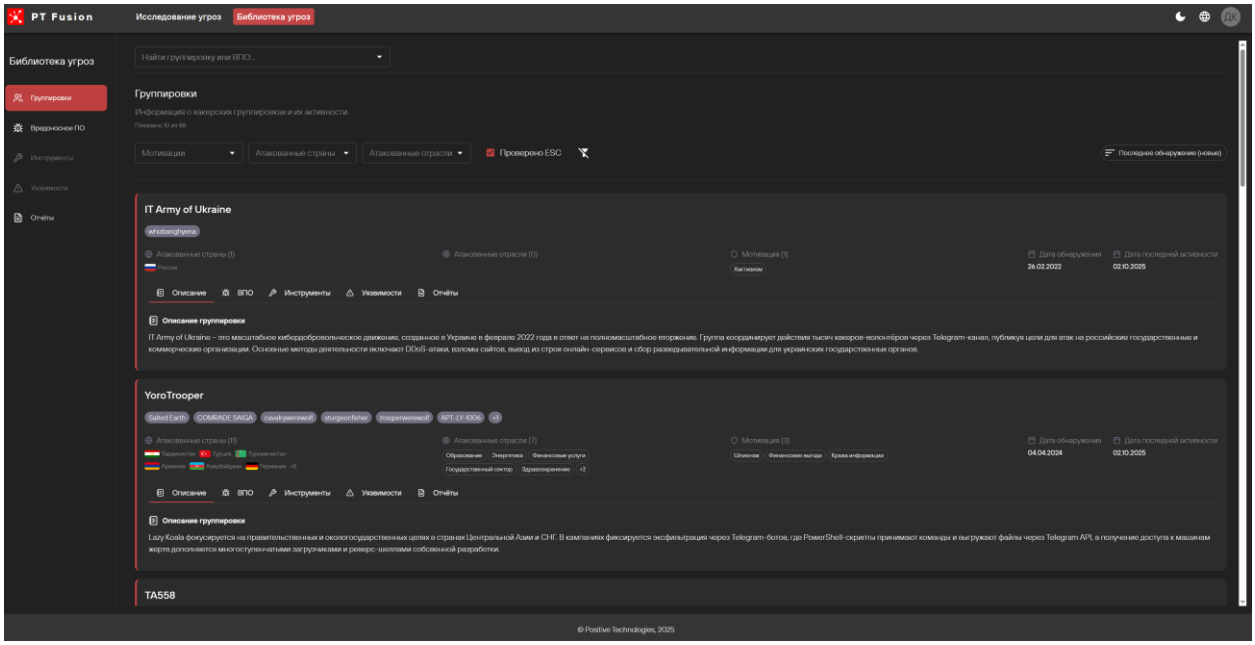

Рисунок 33. Главная страница раздела «Библиотека угроз»

В разделе «Библиотека угроз» представлено 5 подразделов:

- Группировки
- Вредоносное ПО
- Инструменты
- Уязвимости
- Отчеты

Подраздел «Группировки»

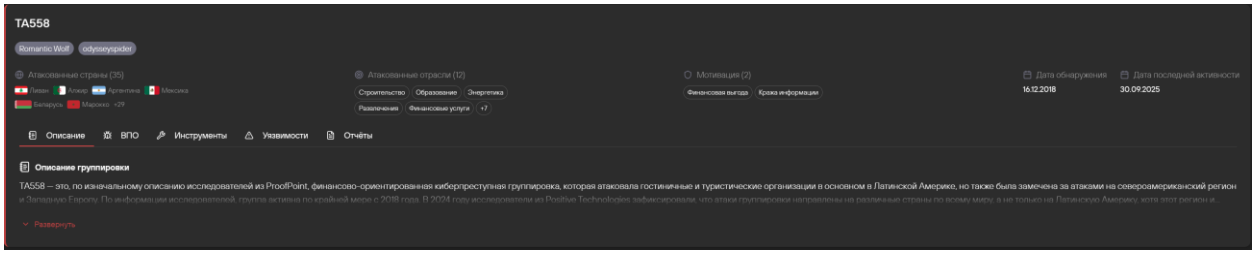

Рисунок 34. Быстрая карточка группировки

В подразделе «Группировки» представлены быстрые карточки с информацией о группировках.

Каждая карточка включает:

- Описание группировки
- Псевдонимы
- Атакованные страны и регионы
- Мотивацию
- Даты первого обнаружения
- Дату последней активности
- Связанные сущности:
  - Используемое ВПО

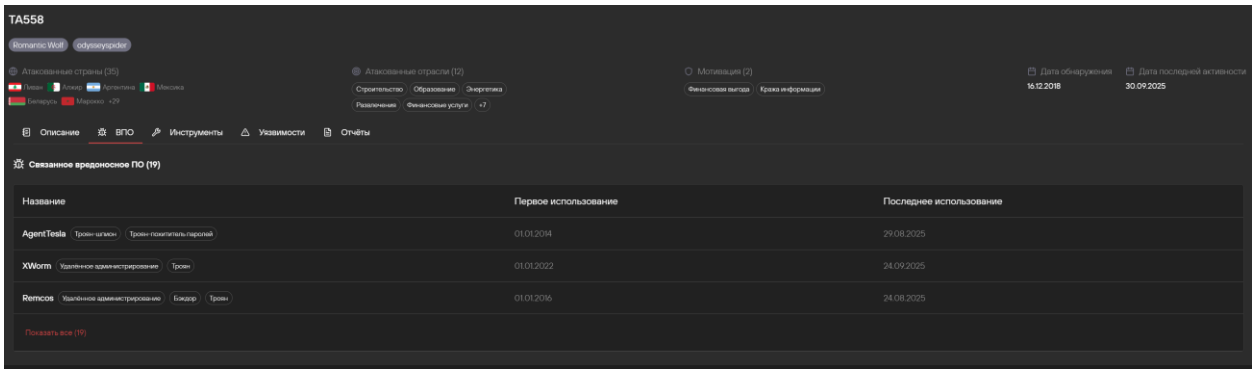

Рисунок 35. Связь с ВПО в быстрой карточке группировки

  - Используемые инструменты

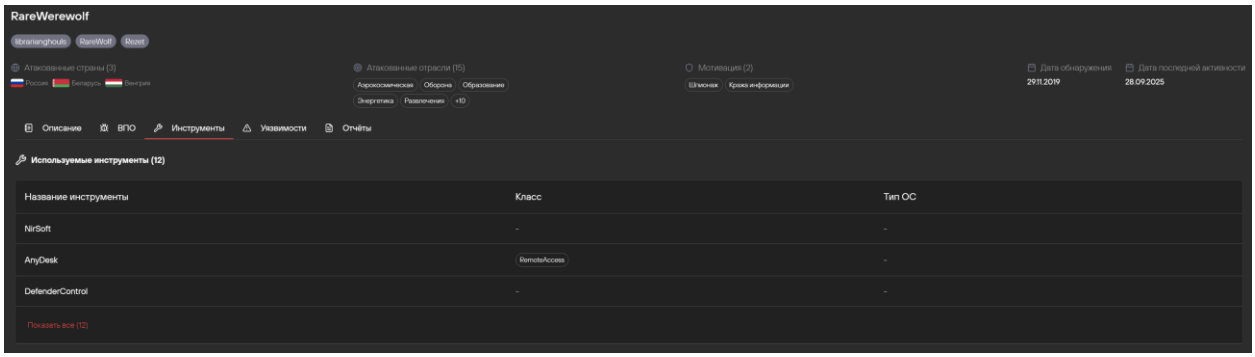

Рисунок 36. Связь с инструментами в быстрой карточке группировки

  - Используемые уязвимости

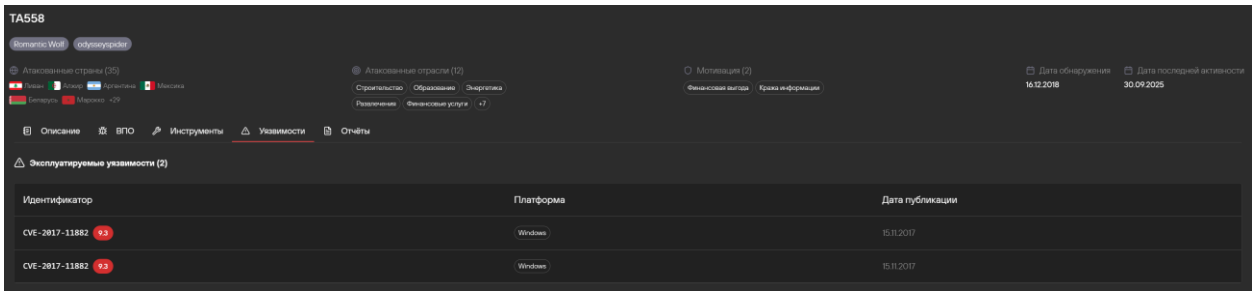

Рисунок 37. Связь с уязвимостями в быстрой карточке группировки

– Связанные публичные отчеты о группировке

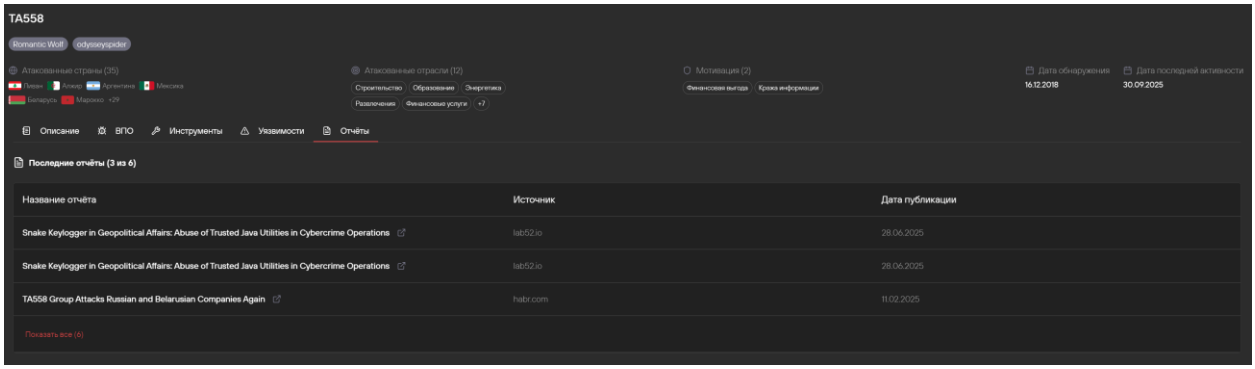

Рисунок 38. Связь с публичными отчетами в быстрой карточке группировки

При нажатии на название группировки пользователь попадет на основную карточку группировки, где можно найти всю туже самую информацию плюс TTP группировки и индикаторы компрометации, которые можно скачать в формате CSV.

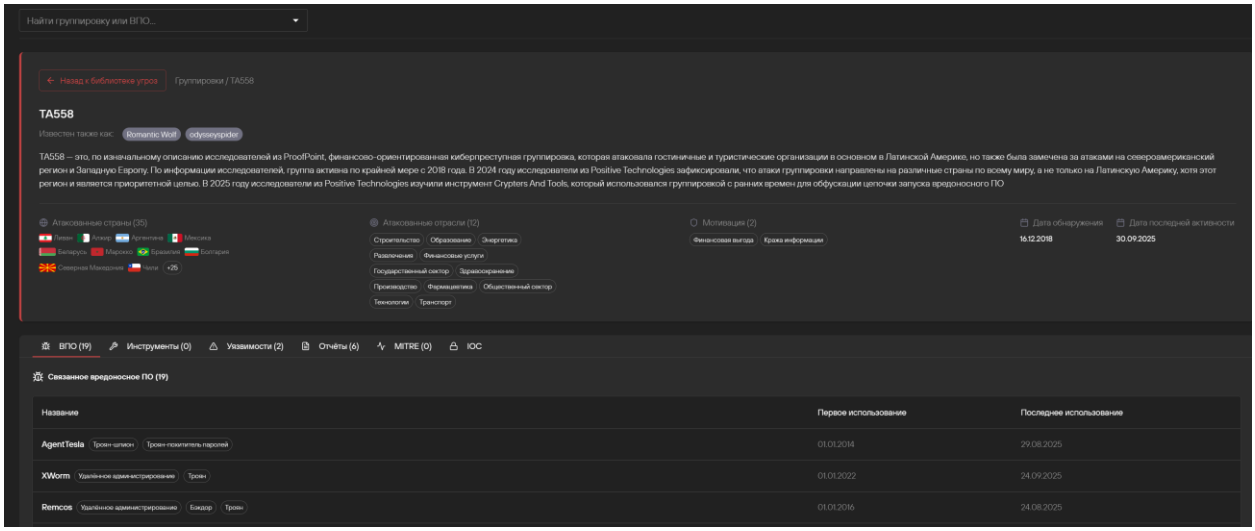

Рисунок 39. Основная карточка группировки

При нажатии на название связанных сущностей пользователь попадает на соответствующую карточку сущности в портале.

В подразделе «Группировки» присутствуют фильтры с помощью, которых пользователь может выбрать группировки, которые имеют определенную мотивацию, атакуют определенные страны и отрасли.

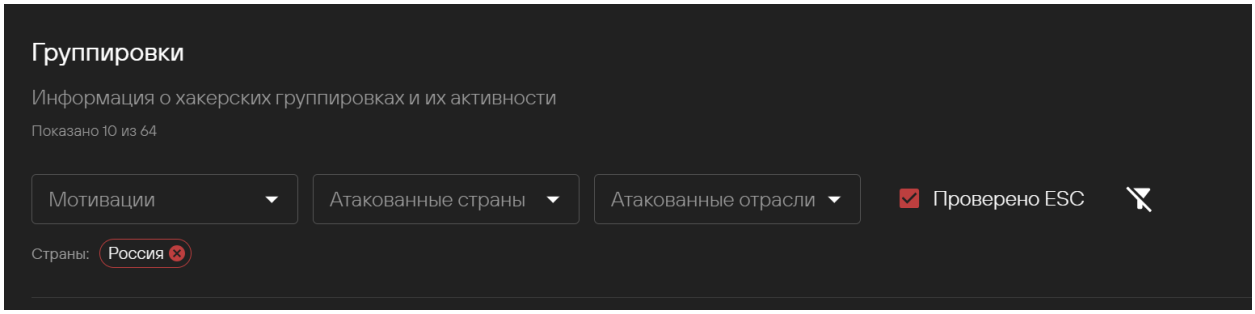

Рисунок 40. Фильтры для подраздела «Группировки»

Также присутствует функционал для отображения всех сущностей, находящихся во внутренней базе, но у них может быть меньше контекста. Для отображения все сущностей необходимо выключить «Проверено ESC».

Подраздел «ВПО»

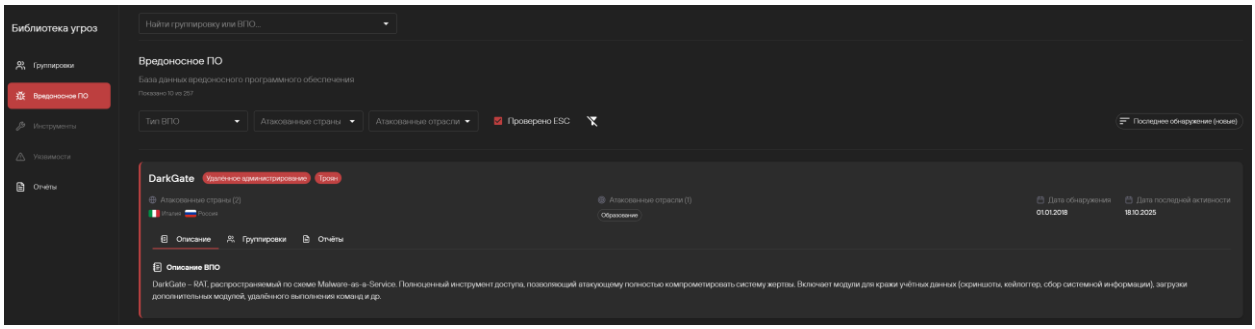

Рисунок 41. Быстрая карточка ВПО

В подразделе «ВПО» представлены быстрые карточки с информацией о вредоносном ПО, которое используют хакерские группировки. Каждая карточка включает:

- Описание ВПО
- Его псевдонимы
- Атакованные страны и регионы
- Даты первого обнаружения
- Дату последней активности
- Связанные сущности:
  - группировки
  - отчеты

При нажатии на название ВПО пользователь попадет на основную карточку ВПО, где можно найти всю туже самую информацию плюс TTP ВПО и индикаторы компрометации, которые можно скачать в формате CSV.

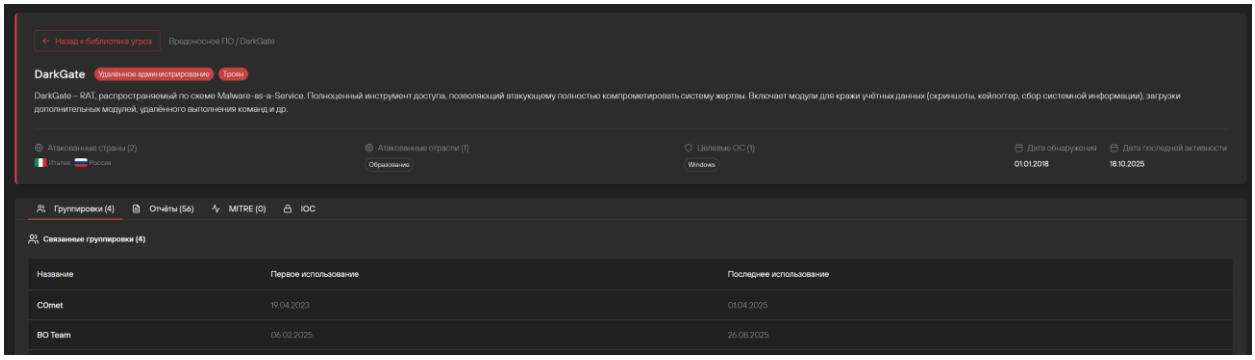

Рисунок 42. Основная карточка ВПО

В подразделе «ВПО» присутствуют фильтры с помощью, которых пользователь может выбрать ВПО, которое используется в атаках на определенные страны и отрасли.

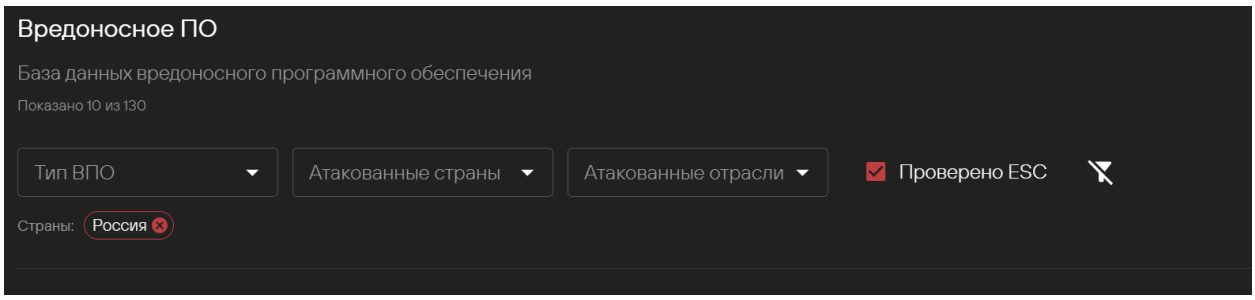

Рисунок 43. Фильтры для подраздела «ВПО»

Также присутствует функционал для отображения всех сущностей, находящихся во внутренней базе, но у них может быть меньше контекста. Для отображения все сущностей необходимо выключить «Проверено ESC».

Подраздел «Отчеты»

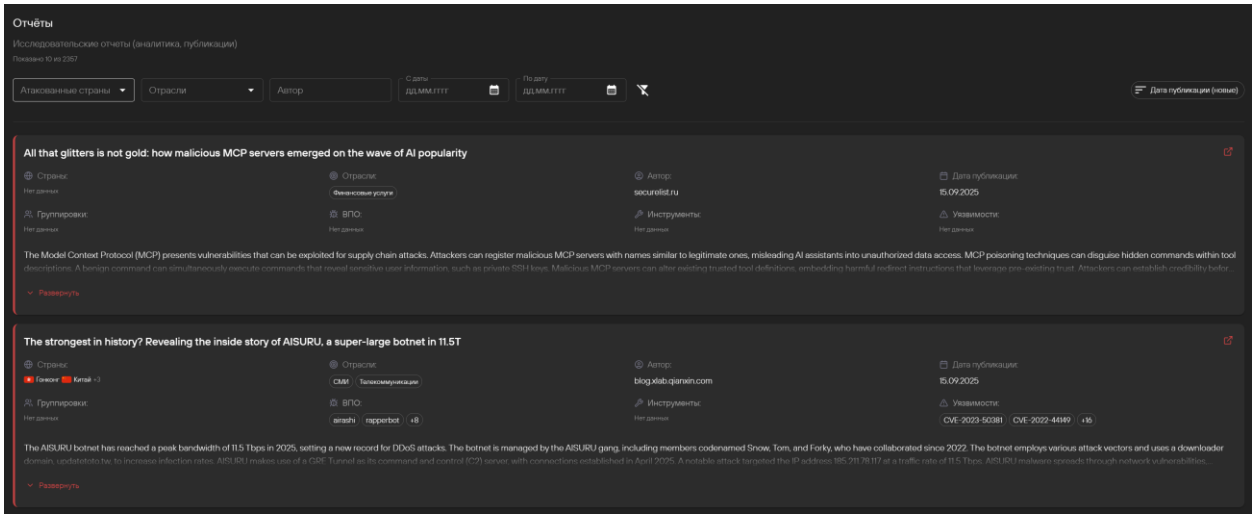

Рисунок 44. Быстрая карточка отчета

В подразделе «Отчеты» представлены быстрые карточки с информацией о публичных отчетах об атаках. Каждая карточка включает:

- Название отчета
- Дату публикации
- Название вендора, опубликовавшего отчет
- Краткое содержание
- Упомянутые атакованные страны
- Упомянутые атакованные отрасли
- Упомянутые группировки
- Упомянутое ВПО
- Упомянутые уязвимости
- Упомянутые инструменты
- Ссылку на отчет

При нажатии на название отчета пользователь попадет на основную карточку отчета, где можно найти всю туже самую информацию.

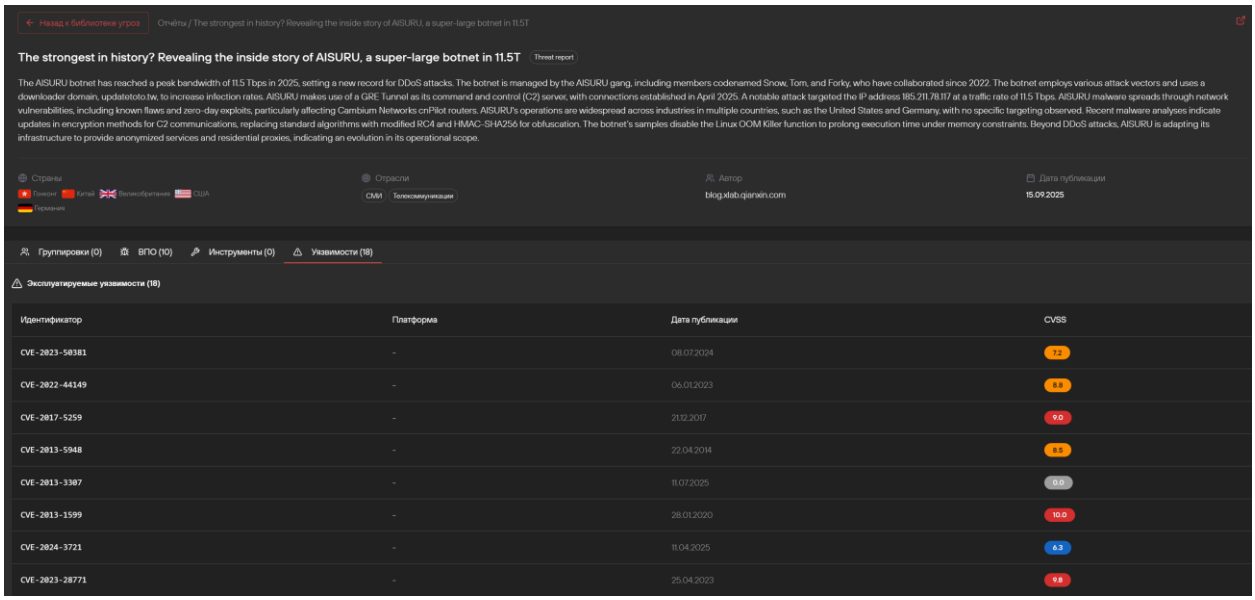

Рисунок 45. Основная карточка отчета

В подразделе «Отчеты» присутствуют фильтры с помощью, которых пользователь может выбрать упомянутые сущности в отчете, вендора, опубликовавшего отчет, а также даты публикации.

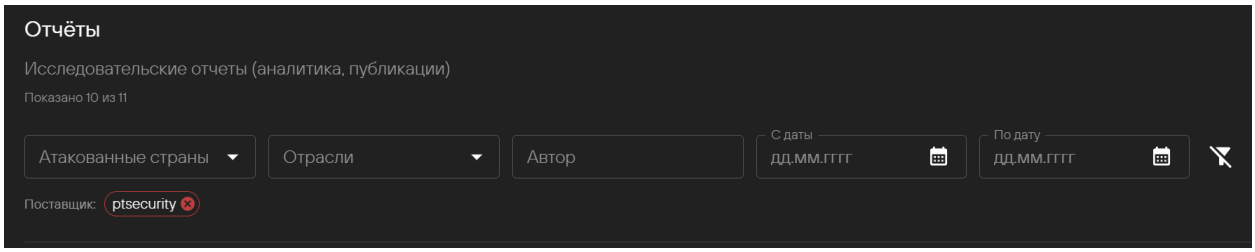

Рисунок 46. Фильтр в подразделе «Отчеты»

8. Личный кабинет

Чтобы войти в личный кабинет в правом верхнем углу экрана нажмите на иконку аккаунта и выберите пункт «Личный кабинет».

В личном кабинете пользователь может изменить название аккаунта, сменить пароль, а также выбрать какой источник географической информации использовать в портале РКН или международный.

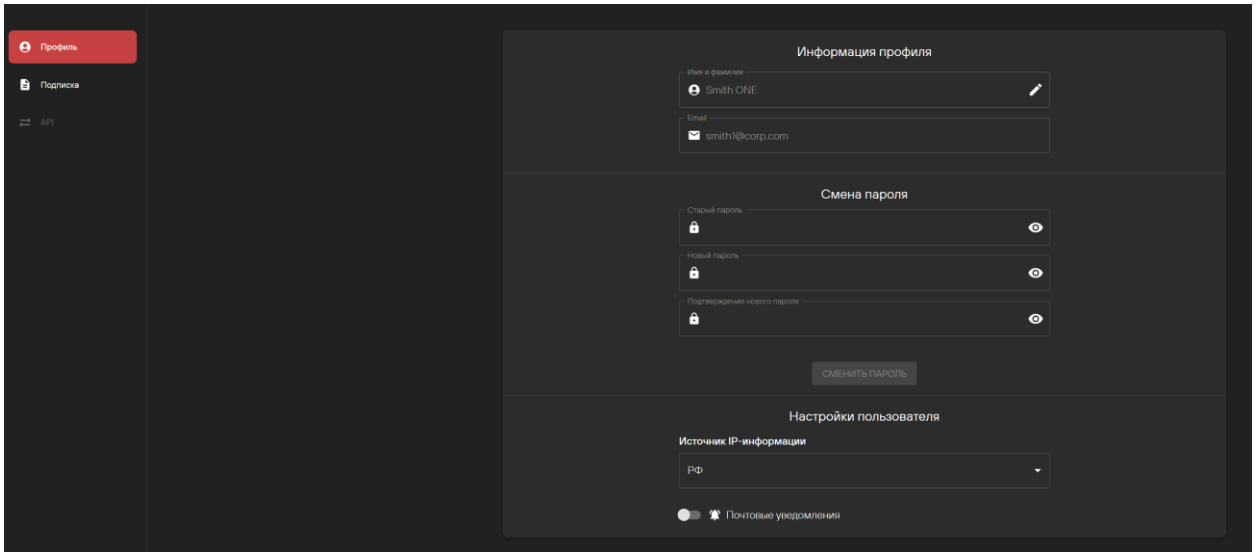

Рисунок 47. Окно изменения информации о пользователе

В личном кабинете так же можно получить информацию о подписке, посмотреть участников подписки и, если пользователь обладает правами «Менеджер подписки», пригласить новых пользователей в свою подписку.

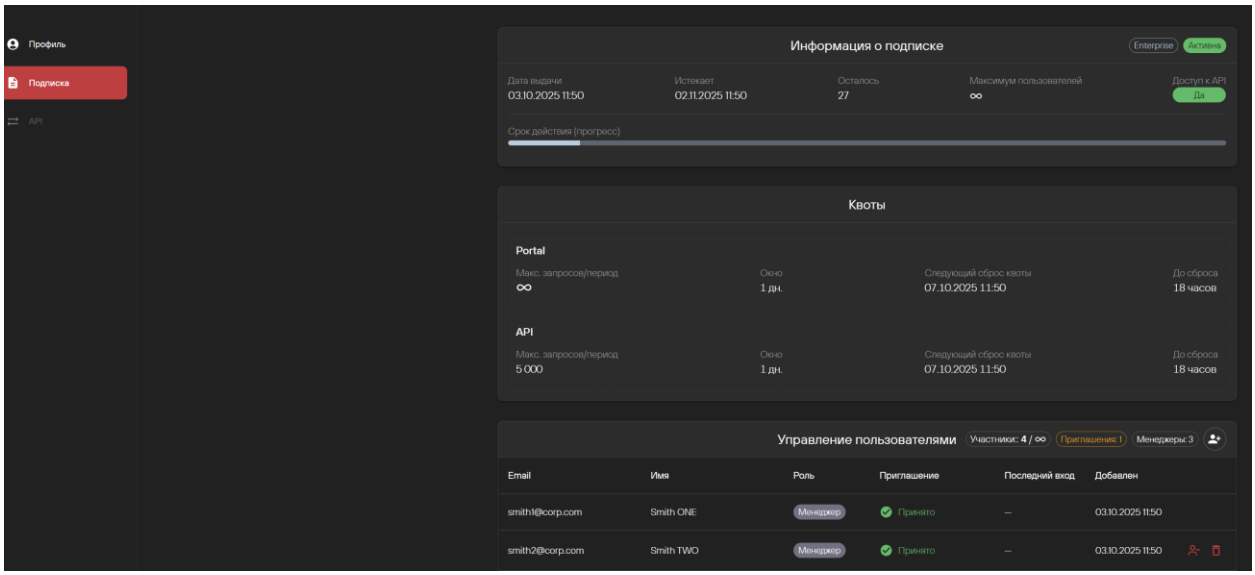

Рисунок 48. Окно получения информации о подписке

9. Обновление и модернизация PT Fusion

Обновление и модернизация PT Fusion выполняются сотрудниками Positive Technologies путем актуализации веб-приложения программы для ЭВМ. В состав новой версии входят добавленные функции и прочие усовершенствования PT Fusion, а также исправления известных проблем предыдущей версии (при наличии).

На странице продукта всегда доступна самая новая версия PT Fusion.

10. Решение проблем

Не удается войти в учетную запись PT Fusion

При попытке входа в учетную запись PT Fusion появляется ошибка. Для решения проверьте правильность имени пользователя и пароля. Если ошибки в данных нет, обратитесь в службу технической поддержки в порядке, описанном в разделе «Обращение в службу технической поддержки (см. раздел 11)».

11. Обращение в службу технической поддержки

Если у вас возникли вопросы или проблемы, вы можете обратиться в техническую поддержку одним из способов:

- написав на почту fusion-support@ptsecurity.com с электронного адреса, который вы указывали при регистрации;
- связавшись с вашим сервисным менеджером.

При обращении приложите файлы, скриншоты и номер задачи. Техническая поддержка оказывается на русском и английском языках.

Запросы в техническую поддержку можно отправлять круглосуточно.

12. Гарантийное обслуживание

Гарантийное обслуживание осуществляют сотрудники компании Positive Technologies.

Условия гарантийного обслуживания определены пользовательским соглашением.

Заявки на гарантийное обслуживание регистрируются через обращение в службу технической поддержки.