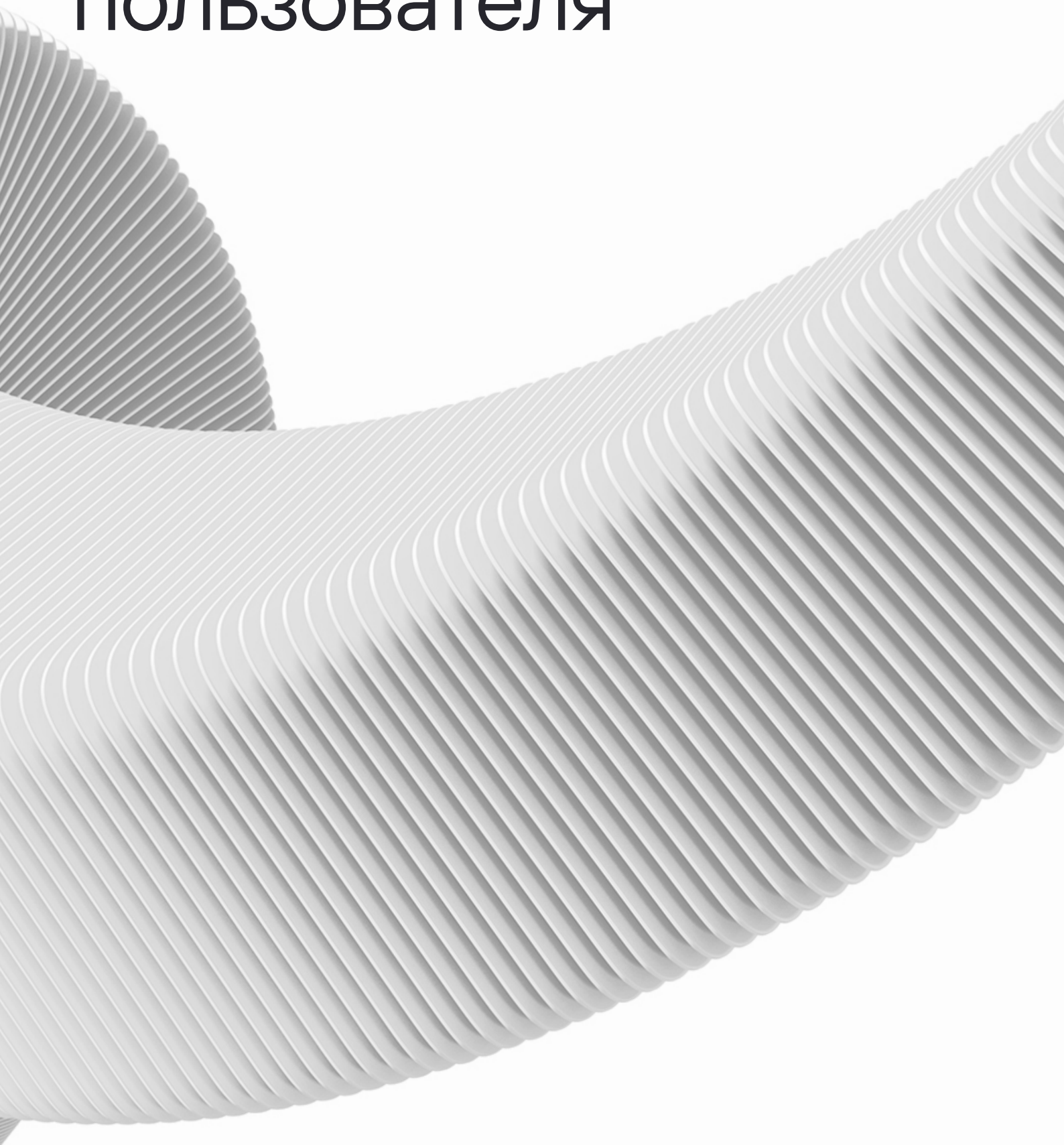


Руководство пользователя



© Positive Technologies, 2025.

Настоящий документ является собственностью Positive Technologies (далее также — Positive Technologies) и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Positive Technologies, pt, PTSECURITY, MaxPatrol, MaxPatrol O2, XSpider, ISIM Industrial Security Incident Manager, SurfPatrol являются зарегистрированными товарными знаками либо товарными знаками Positive Technologies.

Иные товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

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. O 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 portalу;
- 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 раздела 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

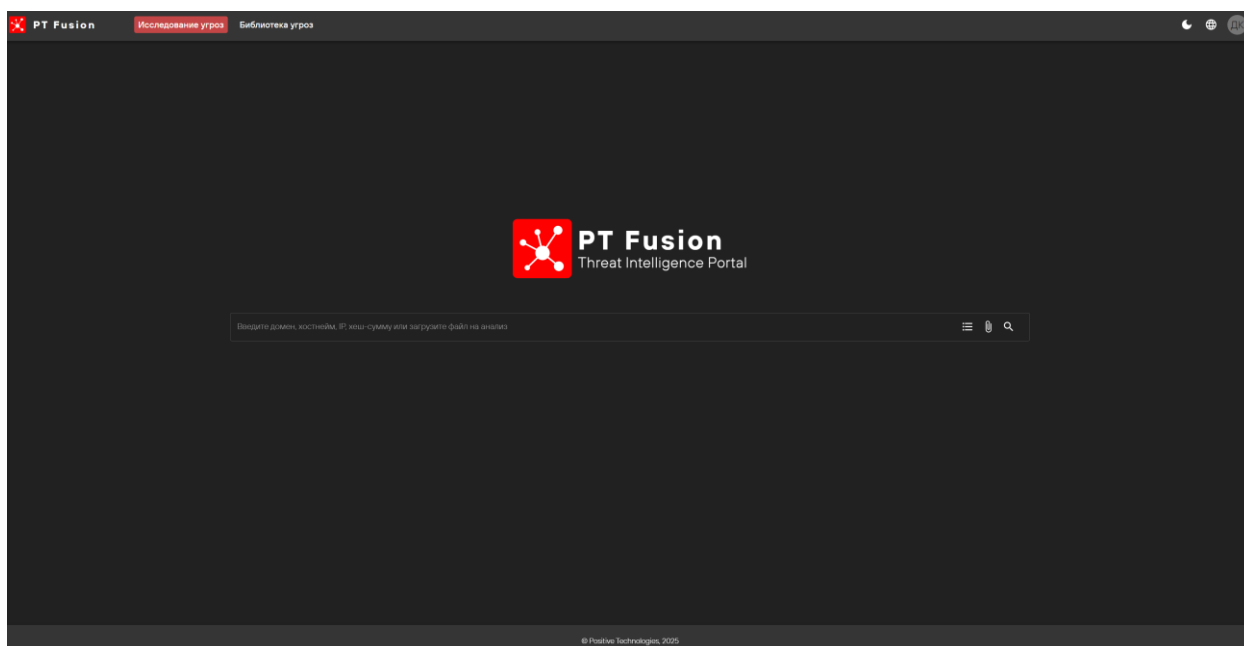


Рисунок 1. Главная страница PT Fusion

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:

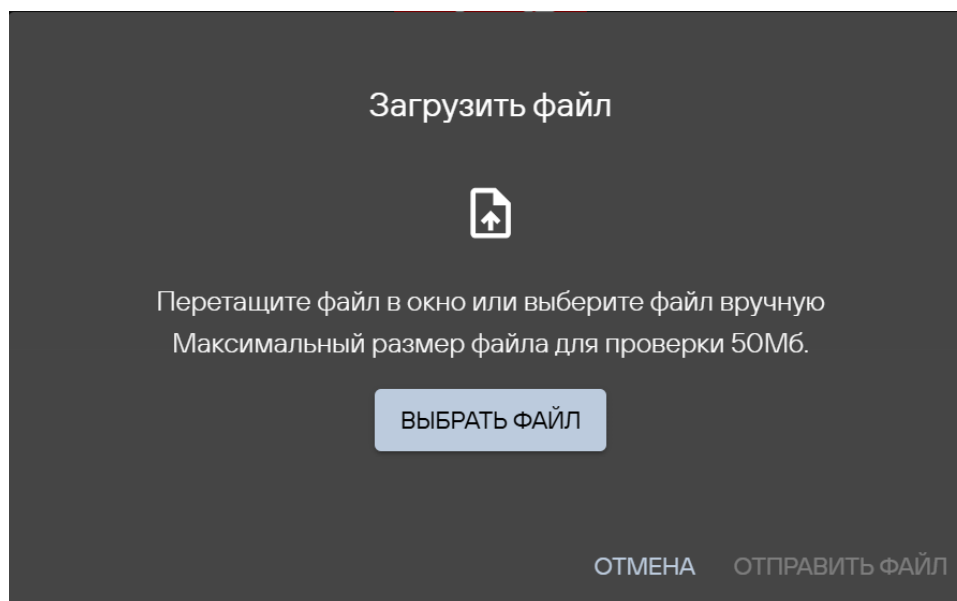


Рисунок 2. Окно загрузки файла

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 параметризованном 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.

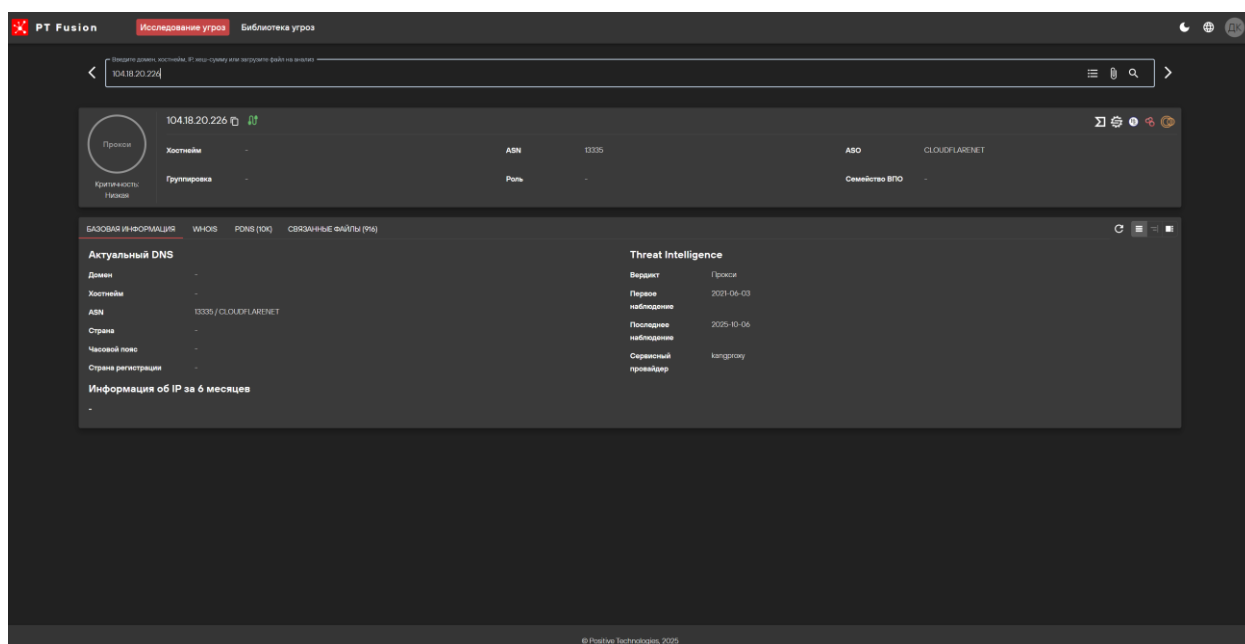


Рисунок 3. Карточка IP адреса

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

Верхний блок

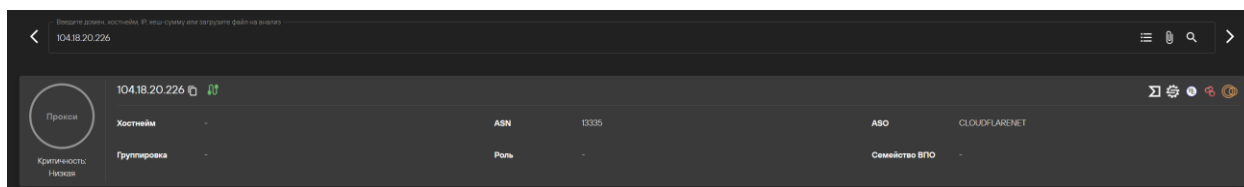


Рисунок 4. Верхняя карточка IP адреса

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.

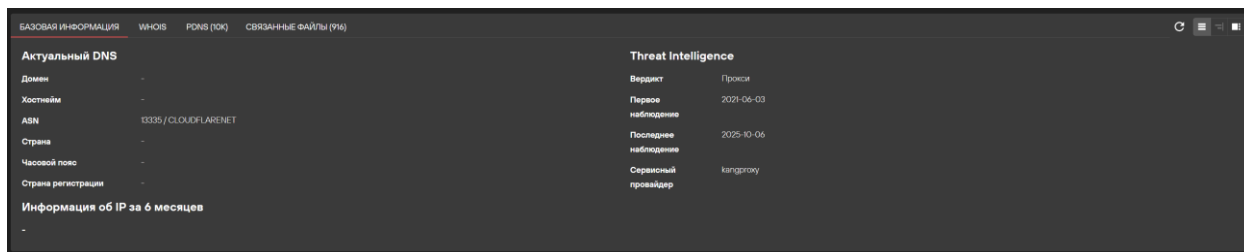


Рисунок 5. Нижний блок карточки IP адреса

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.

БАЗОВАЯ ИНФОРМАЦИЯ

WHOIS

PNDS (10K)

СВЯЗАННЫЕ ФАЙЛЫ (916)

Зарегистрирован

2014-03-28

Ключевые события

last changed

2024-09-04

Срок действия истекает

-

registration

2014-03-28

Диапазон IP-адресов

104.16.0.0 - 104.31.255.255

Текущий статус

active

Имя сети

CLOUDFLARENET

Контакты

Наименование

Организация

Адрес электронной почты

Телефон

Страна

Регион

Населенный пункт

Почтовый код

Улица

ИИН

Registrar

-

-

-

-

-

-

-

-

-

Registrant

Cloudflare, Inc.

-

-

-

-

-

-

-

-

Admin

-

-

-

-

-

-

-

-

-

Abuse

Abuse

Abuse

abuse@cloudflare.com

+1-650-319-8930

-

-

-

-

-

Tech

Admin

Admin

rs@cloudflare.com

+1-650-319-8930

-

-

-

-

-

Показать исходный формат WHOIS данных

Рисунок 6. Карточка WHOIS IP адреса

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

БАЗОВАЯ ИНФОРМАЦИЯ

WHOIS

PNDS (10K)

СВЯЗАННЫЕ ФАЙЛЫ (916)

Тип

Домен

Хостнейм

GEO

Первое наблюдение

Последнее наблюдение

a

msging.net

wacademy.wa.msging.net

ASN: 13335
ASO: CLOUDFLARENET
GEO: -

2025-03-07

2025-10-06

a

msging.net

product.wa.gw.msging.net

ASN: 13335
ASO: CLOUDFLARENET
GEO: -

2024-10-17

2025-10-06

a

msging.net

lidercap.http.msging.net

ASN: 13335
ASO: CLOUDFLARENET
GEO: -

2025-02-11

2025-10-06

a

msging.net

prefeiturafranca.http.msging.net

ASN: 13335
ASO: CLOUDFLARENET
GEO: -

2024-08-25

2025-10-06

a

msging.net

incotrading.wa.gw.msging.net

ASN: 13335
ASO: CLOUDFLARENET
GEO: -

2024-11-15

2025-10-06

a

msging.net

smartfict.http.msging.net

ASN: 13335
ASO: CLOUDFLARENET
GEO: -

2025-03-13

2025-10-06

a

msging.net

fcagroup.http.msging.net

ASN: 13335
ASO: CLOUDFLARENET
GEO: -

2024-06-18

2025-10-06

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.

БАЗОВАЯ ИНФОРМАЦИЯ

WHOIS

PNDS (10K)

СВЯЗАННЫЕ ФАЙЛЫ (916)

Тип запроса

Домен

Хостнейм

ASN

ASO

GEO

Диапазон дат

Хостнейм

msging.net

msging.net

msging.net

wasaca

produ

lidero

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.

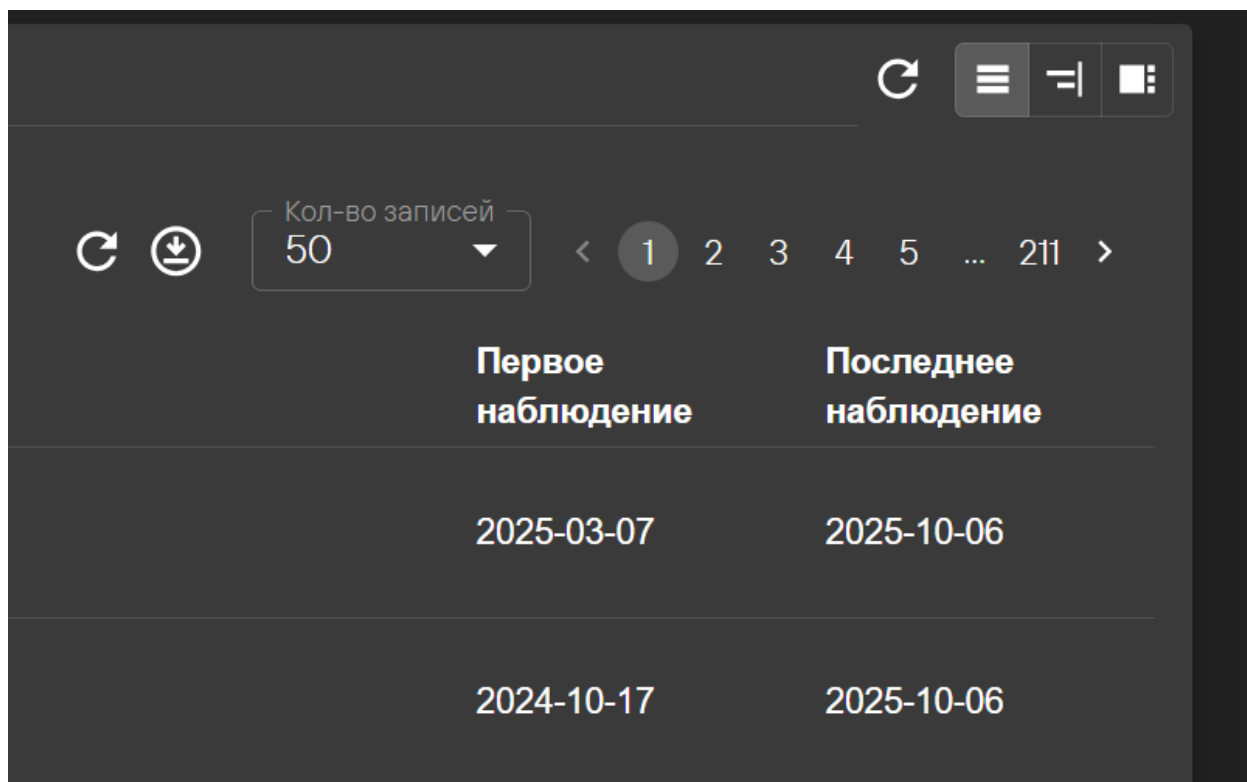


Рисунок 9. Кнопки переключения отображения представлений, отображение сводки и скачивания результата поиска в PDNS в CSV формате

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.

Сводка	
Вердикт	
Не определен	10486
Чистый	10050
Безопасный	305
Вероятно опасный	9
CRL/OCSP узел	4
Рекламный сервер	2
DynDNS хостинг	2
ASN	
13335	10518
Домены	
identitynow-demo.com	4833
msging.net	4015

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 IP присутствует в извлеченной конфигурации ВПО.

БАЗОВАЯ ИНФОРМАЦИЯ WHOIS PDNS (ПК) СВЯЗАННЫЕ ФАЙЛЫ (ПК)							
СВЯЗАННЫЕ ФАЙЛЫ (916)							
Имя	Тип	Размер файла	Группировка	Семейство	Класс ВПО	Первое наблюдение	Последнее наблюдение
94917.exe	pe	344.55 KB	-	Morstar	RiskTool	2025-05-26	2025-10-02
94338.exe	pe	344.57 KB	-	-	RiskTool	2025-05-23	2025-10-01
61a63246d7f4e0c3488a0c26480c03e7860483919577347d9e72ab0c794f	pe	225.66 KB	-	-	-	2024-10-21	2025-09-29
2025-09-29_29748d45ca118a31c1113a71898c0cda_cstrminer_exe_ha	pe	225.66 KB	-	-	-	2025-09-29	2025-09-29
29_29748d45ca118a31c1113a71898c0cda_cstrminer_exe_ha	pe	225.66 KB	-	-	-	2025-09-29	2025-09-29
ashampoo_driver_updater_1.9.0.exe	pe	12.16 MB	-	Emotet	Trojan-Downloader	2025-08-01	2025-09-28
4ja58fk.exe	pe	10.13 MB	-	Tedy	Trojan-PSW	2025-08-22	2025-09-27
NetLimiter v5.3.25.exe	pe	5.93 MB	-	AdLoad	Trojan	2025-06-28	2025-09-23
netlimiter-5.3.23.0 (1).exe	pe	10.27 MB	-	-	-	2025-03-21	2025-09-17

Рисунок 12. Вкладка со связанными файлами

БАЗОВАЯ ИНФОРМАЦИЯ WHOIS PDNS (ПК) СВЯЗАННЫЕ ФАЙЛЫ (ПК)							
СВЯЗАННЫЕ ФАЙЛЫ (3800) СВЯЗАННЫЕ ФАЙЛЫ ЧЕРЕЗ КОНТЕЙНЕР (1423)							
Имя	Тип	Размер файла	Группировка	Семейство	Класс ВПО	Первое наблюдение	Последнее наблюдение
AMD Processor.exe	exe	1.43 MB	-	Nanocore	-	2025-07-02	2025-07-05
C:\Users\<USER>\AppData\Roaming\app.exe	exe	1.74 MB	-	Nanocore	-	2025-08-14	2025-08-14
AMD Processor.exe	exe	1.06 MB	-	Nanocore	-	2025-07-09	2025-07-13
dfcodexgas.7137cfa5a86b619489302a7a89d5af4ed8	exe	1.32 MB	-	Nanocore	-	2025-06-16	2025-06-30
AMD Processor.exe	exe	1.75 MB	-	Nanocore	-	2025-06-17	2025-07-01
C:\Users\<USER>\AppData\Roaming\app.exe	exe	1018.11 KB	-	Nanocore	-	2025-06-08	2025-06-19
C:\Users\<USER>\AppData\Roaming\app.exe	exe	1.79 MB	-	Nanocore	-	2025-08-14	2025-08-14
dfcodexgas.b8a58deca48577c7444476472002911470c5	exe	1.72 MB	-	Nanocore	-	2025-08-13	2025-08-16
dfcodexgas.008b107486a00c7a7d0811a11d8ce358515	exe	1.80 MB	-	Nanocore	-	2025-06-14	2025-06-27

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:

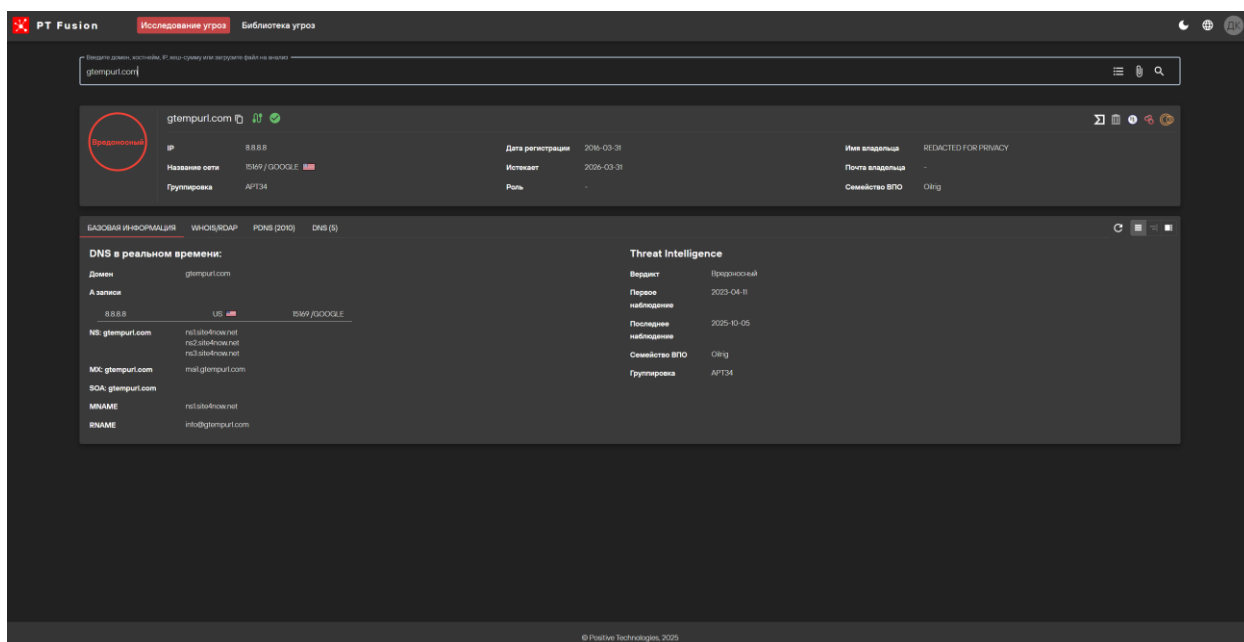


Рисунок 14. Карточка домена/хостнейма

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

Верхний блок

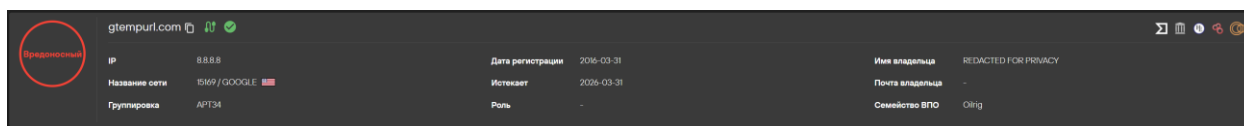


Рисунок 15. Верхний блок карточки домена/хостнейма

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 ocsf	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/202500000000000*/
- 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.

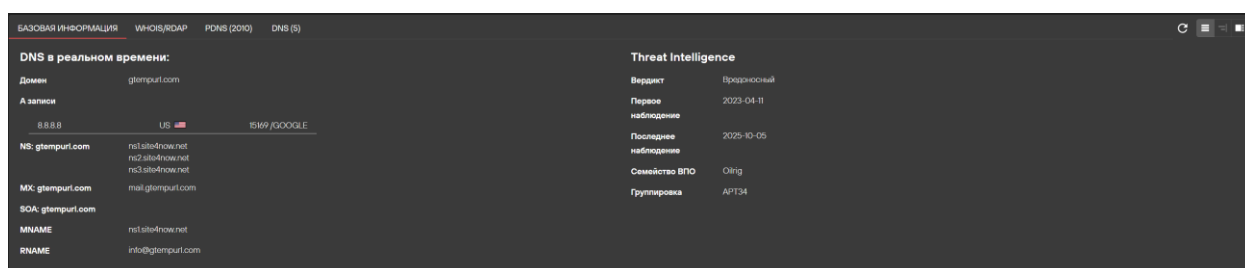


Рисунок 16. Нижний блок карточки домена/хостнейма. Базовая информация

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

БАЗОВАЯ ИНФОРМАЦИЯWHOIS/RDAPPDNS (2010)DNS (5)

WHOIS

ИСТОРИЧЕСКИЙ WHOIS

ИСТОРИЧЕСКИЙ RDAP

Домен

glampurl.com

Зарегистрирован

2016-03-31

Срок действия истекает

2026-03-31

Ключевые события

registration

2016-03-31

expiration

2026-03-31

last changed

2025-01-11

Текущий статус

ok

Контакты	Наименование	Организация	Адрес электронной почты	Телефон	Страна	Регион	Населенный пункт	Почтовый код	Улица	ИНН
Registrar	TUCOWS DOMAINS, INC.	-	domainabuse@tucows.com	+141635023	-	-	-	-	-	-
Registrant	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY	https://redaccess.com/contact/a390b333-8b60-44cd-b896-99ba546d8ab	REDACTED FOR PRIVACY	HK	HK	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY	REDACTED FOR PRIVACY	-
Admin	-	-	-	-	-	-	-	-	-	-
Abuse	-	-	-	-	-	-	-	-	-	-
Tech	-	-	-	-	-	-	-	-	-	-

Показать исходный формат WHOIS данных

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.

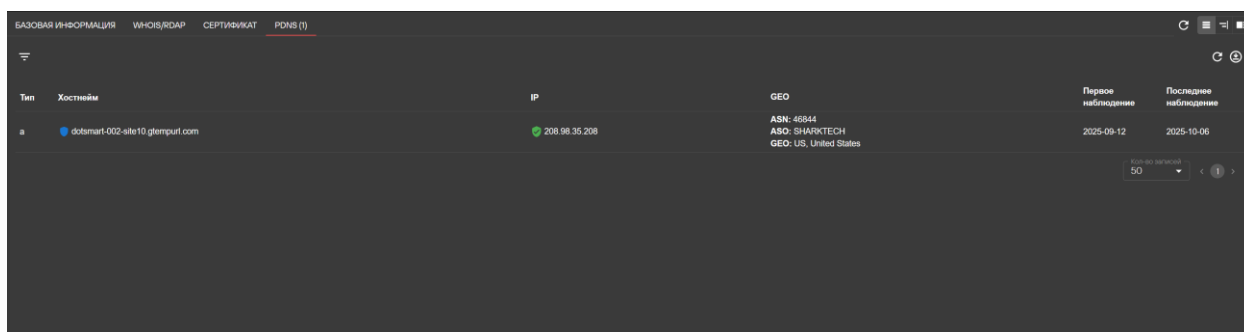
БАЗОВАЯ ИНФОРМАЦИЯ WHOIS/RDAP PDNS (2010) DNS (5)									
ДОМЕН (1) ХОСТНЕЙМЫ (2009)									
Тип	Домен	IP	GEO			Первое наблюдение	Последнее наблюдение		
a	glampurl.com	8.8.8.8	ASN: 15169	ASO: GOOGLE	GEO: US, United States	2025-08-06	2025-09-30	Всего записей: 50	1

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

БАЗОВАЯ ИНФОРМАЦИЯ WHOIS/RDAP PDNS (2010) DNS (5)									
ДОМЕН (1) ХОСТНЕЙМЫ (2009)									
Тип	Хостнейм	IP	GEO			Первое наблюдение	Последнее наблюдение		
a	dotsmart-002-site10.glampurl.com	208.98.35.208	ASN: 46844	ASO: SHARKTECH	GEO: US, United States	2025-09-12	2025-10-06		
a	jcastiloro-001-site1.glampurl.com	208.98.35.196	ASN: 46844	ASO: SHARKTECH	GEO: US, United States	2025-09-05	2025-10-06		
a	hwwg1-001-site1.glampurl.com	208.98.35.80	ASN: 46844	ASO: SHARKTECH	GEO: US, United States	2024-09-03	2025-10-06		
a	relishcloud-001-site19.glampurl.com	208.98.35.229	ASN: 46844	ASO: SHARKTECH	GEO: US, United States	2024-09-10	2025-10-06		
a	taletbank-001-site1.glampurl.com	208.98.35.197	ASN: 46844	ASO: SHARKTECH	GEO: US, United States	2024-09-17	2025-10-06		
a	dotsmart-003-site9.glampurl.com	70.39.90.16	ASN: 46844	ASO: SHARKTECH	GEO: US, United States	2024-08-10	2025-10-05		

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

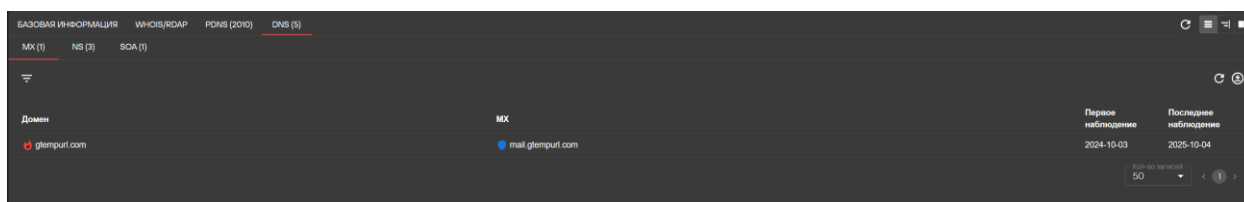
При запросе хостнейма вкладка PDNS будет отображен PDNS только запрошенного хостнейма.



Тип	Хостнейм	IP	GEO	Первое наблюдение	Последнее наблюдение
a	dotsmart-002-site10.gltempurl.com	208.98.35.208	ASN: 46844 ASO: SHARKTECH GEO: US, United States	2025-09-12	2025-10-06

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

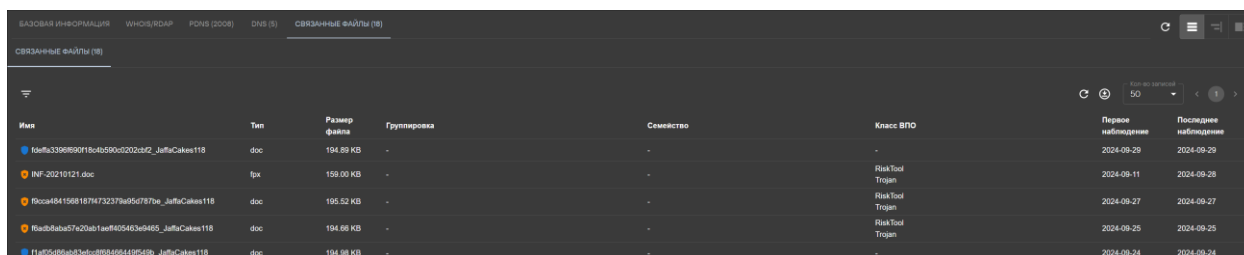
DNS – вкладка содержит информацию о NS, MX и SOA записях домена или хостнейма.



Домен	MX	Первое наблюдение	Последнее наблюдение
gltempurl.com	mail.gltempurl.com	2024-10-03	2025-10-04

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.



Имя	Тип	Размер файла	Группировка	Семейство	Класс ВПО	Первое наблюдение	Последнее наблюдение
ba9fa3396860f1b4b590d202d3f2_jaffaCakes118	doc	194.69 KB	-	-	-	2024-09-29	2024-09-29
BNF-20210121.doc	txt	159.00 KB	-	-	RiskTool Trojan	2024-09-11	2024-09-28
fbcc4641568187473237a9d5d787be_jaffaCakes118	doc	195.52 KB	-	-	RiskTool Trojan	2024-09-27	2024-09-27
ba9fa3396860f1b4b590d202d3f2_jaffaCakes118	doc	194.66 KB	-	-	RiskTool Trojan	2024-09-25	2024-09-25
f1a05d9bab3efc08b0466440549b_jaffaCakes118	doc	194.98 KB	-	-	-	2024-09-24	2024-09-24

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.

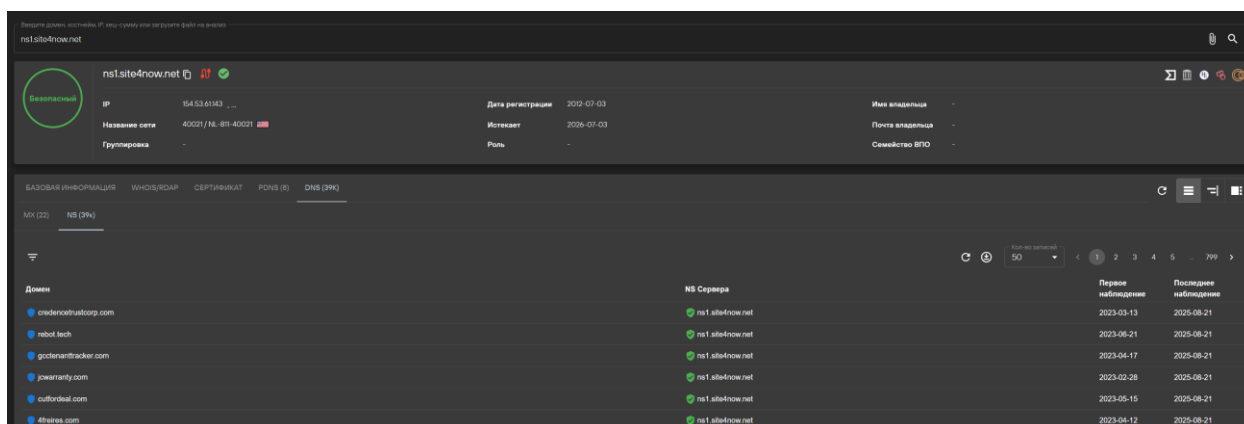


Рисунок 23. Пример поиска по NS Записи

Результаты поиска по хеш-суммам

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

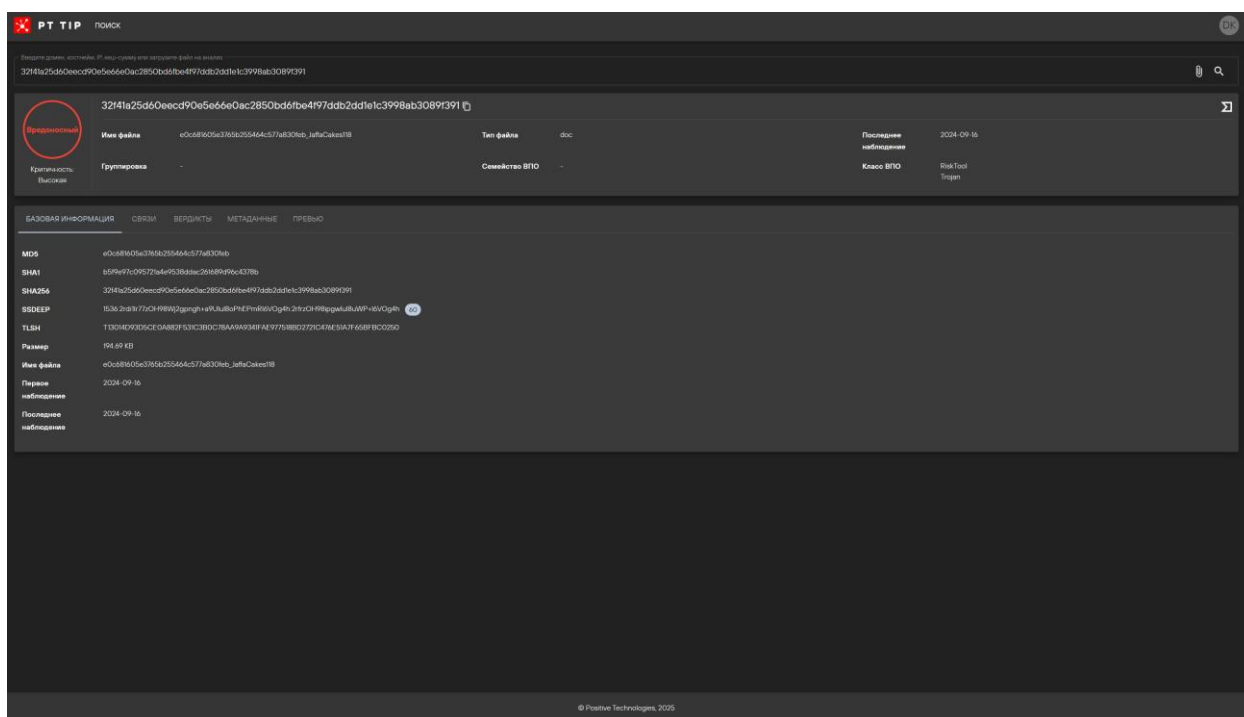


Рисунок 24. Результат поиска по хеш-сумме

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

Верхний блок

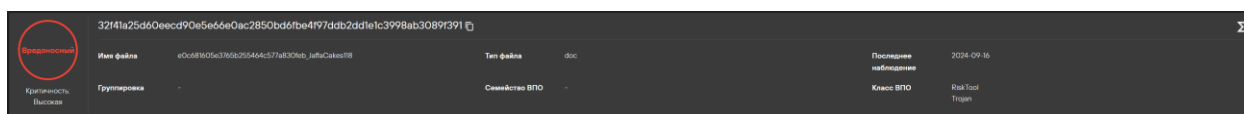


Рисунок 25. Верхний блок карточки хеш-суммы

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.

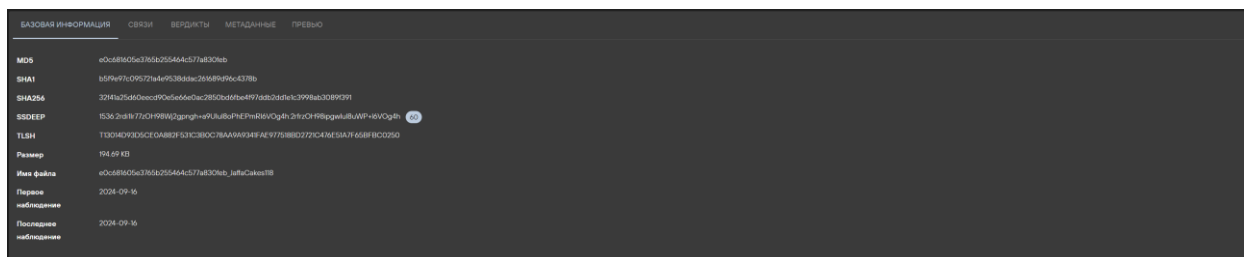


Рисунок 26. Нижний блок карточки хеш-суммы

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

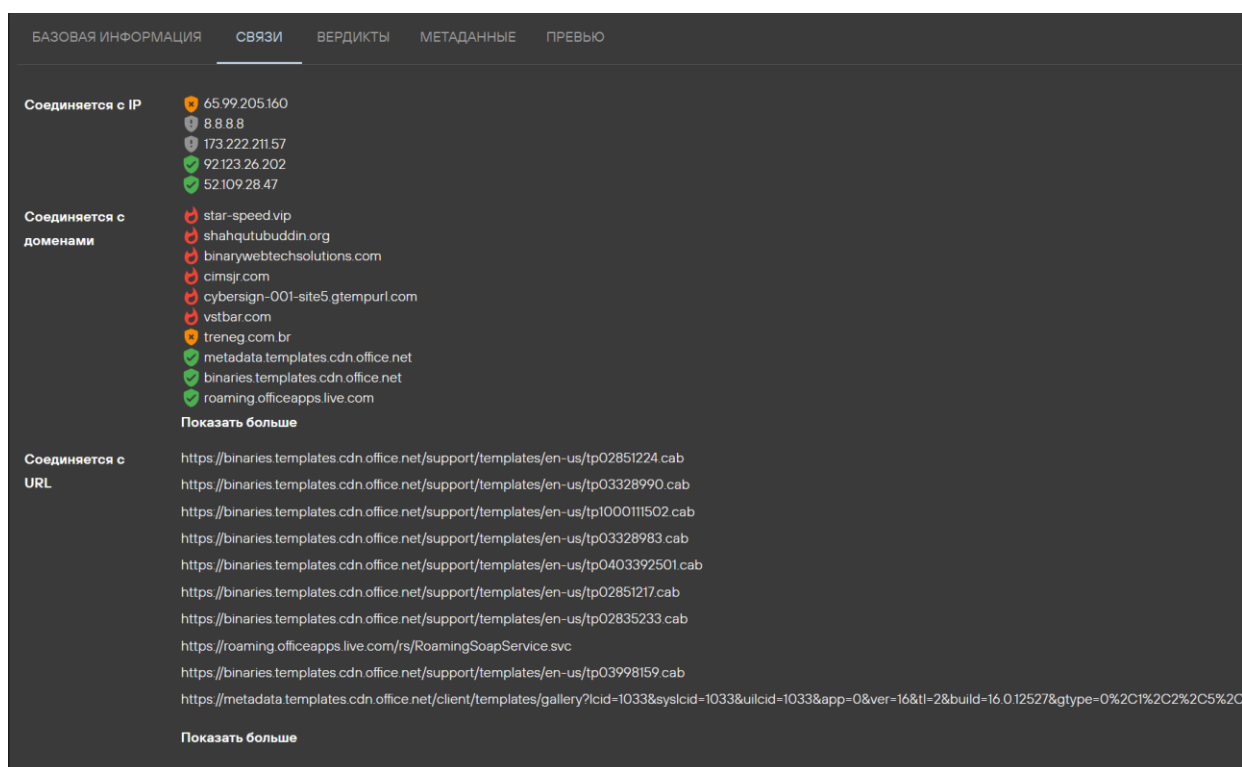


Рисунок 27. Связи файла с другими индикаторами

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

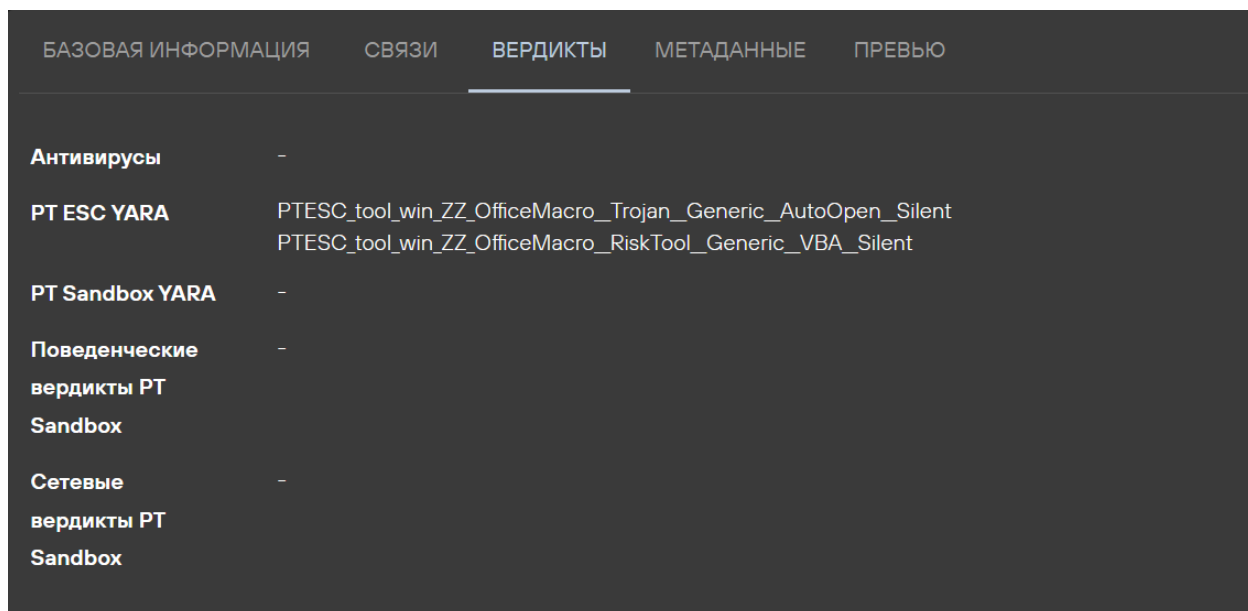


Рисунок 28. Вердикты на файл

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

БАЗОВАЯ ИНФОРМАЦИЯ		СВЯЗИ	ВЕРДИКТЫ	МЕТАДАННЫЕ	ПРЕВЬЮ
Автор	Mélissa Perez				
Заголовок	Aut.				
Приложение	Microsoft Office Word				
Версия	15.0				
Ревизия	1				
Шаблон	Normal.dotm				
Кодировка	Unicode UTF-16, little endian				
Язык	English				
Количество страниц	2				
Количество параграфов	1				
Количество строк	1				
Количество слов	4				
Количество букв	24				
Количество символов	27				
Дата создания	2020-09-18T21:15:00				
Дата изменения	2020-09-18T21:15:00				
Флаги	Has picture Table ExtChar				

Рисунок 29. Метаданные файла

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

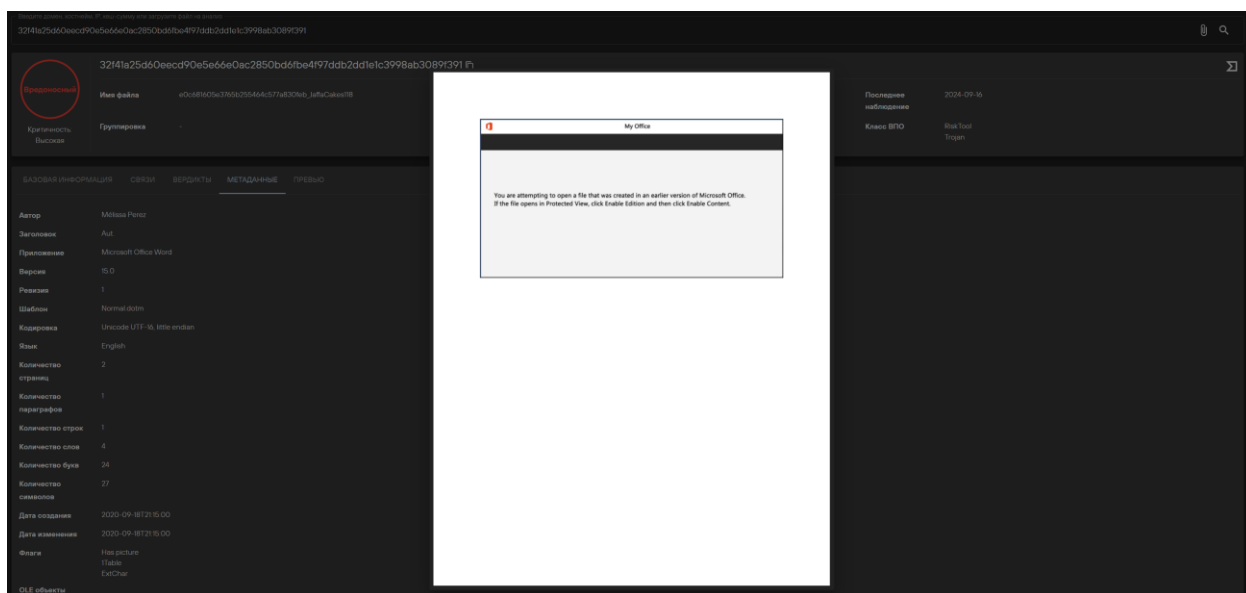
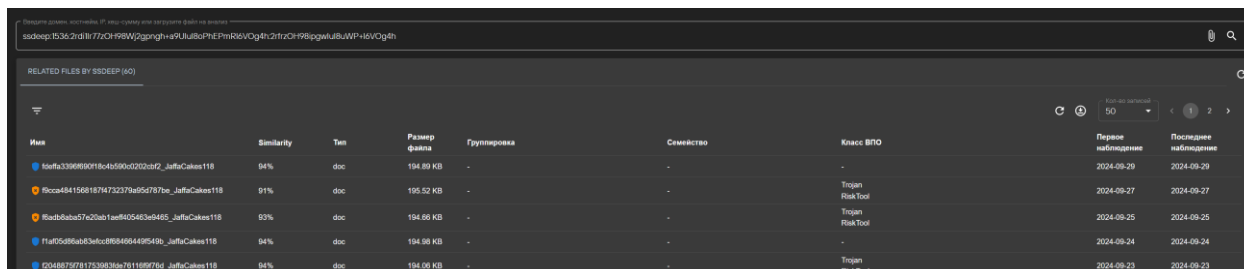


Рисунок 30. Превью файла

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.



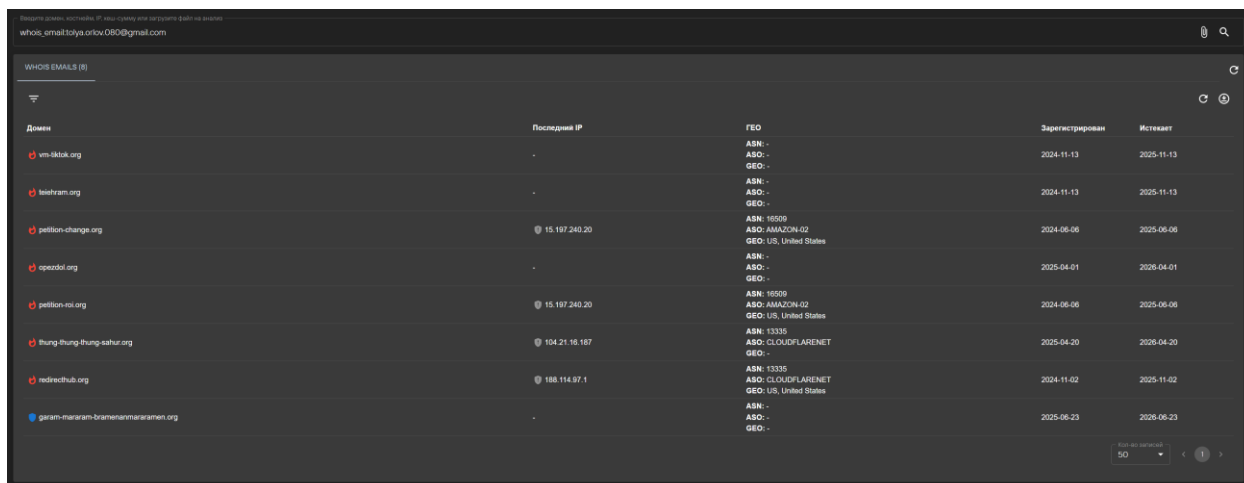
Имя	Similarity	Тип	Размер файла	Группировка	Семейство	Класс ВПО	Первое наблюдение	Последнее наблюдение
5a6fa3396909f18c4d590c020c8f2_jaffaCakes118	94%	doc	194.89 KB	-	-	-	2024-09-29	2024-09-29
9cc48415081874732379ad54787be_jaffaCakes118	91%	doc	195.52 KB	-	-	Trojan RiskTool	2024-09-27	2024-09-27
8a6b8ba57a20ab1ae8f05463e4495_jaffaCakes118	93%	doc	194.66 KB	-	-	Trojan RiskTool	2024-09-25	2024-09-25
f1a05d8ba63efcc88469449549b_jaffaCakes118	94%	doc	194.98 KB	-	-	-	2024-09-24	2024-09-24
0048879781753983da761168f76d_jaffaCakes118	94%	doc	194.06 KB	-	-	Trojan RiskTool	2024-09-23	2024-09-23

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 ящику можно, как через поисковую строку с помощью параметра «whois_email:» или же нажав почтовый ящик регистранта в нижней карточке, во вкладке WHOIS/RDAP



Домен	Последняя IP	ГЕО	Зарегистрирован	Истекает
vm-ibkuk.org	-	ASN: - ASO: - GEO: -	2024-11-13	2025-11-13
teahram.org	-	ASN: - ASO: - GEO: -	2024-11-13	2025-11-13
petition-change.org	15.197.240.20	ASN: 16509 ASO: AMAZON-02 GEO: US, United States	2024-06-06	2025-06-06
opendol.org	-	ASN: - ASO: - GEO: -	2025-04-01	2026-04-01
petition-rol.org	15.197.240.20	ASN: 16509 ASO: AMAZON-02 GEO: US, United States	2024-06-06	2025-06-06
thung-thung-sahur.org	104.21.15.167	ASN: 13335 ASO: CLOUDFLARENET GEO: -	2025-04-20	2026-04-20
redirecthub.org	188.114.97.1	ASN: 13335 ASO: CLOUDFLARENET GEO: US, United States	2024-11-02	2025-11-02
garim-mararam-bramenamaramen.org	-	ASN: - ASO: - GEO: -	2025-06-23	2026-06-23

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 метаданных 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.

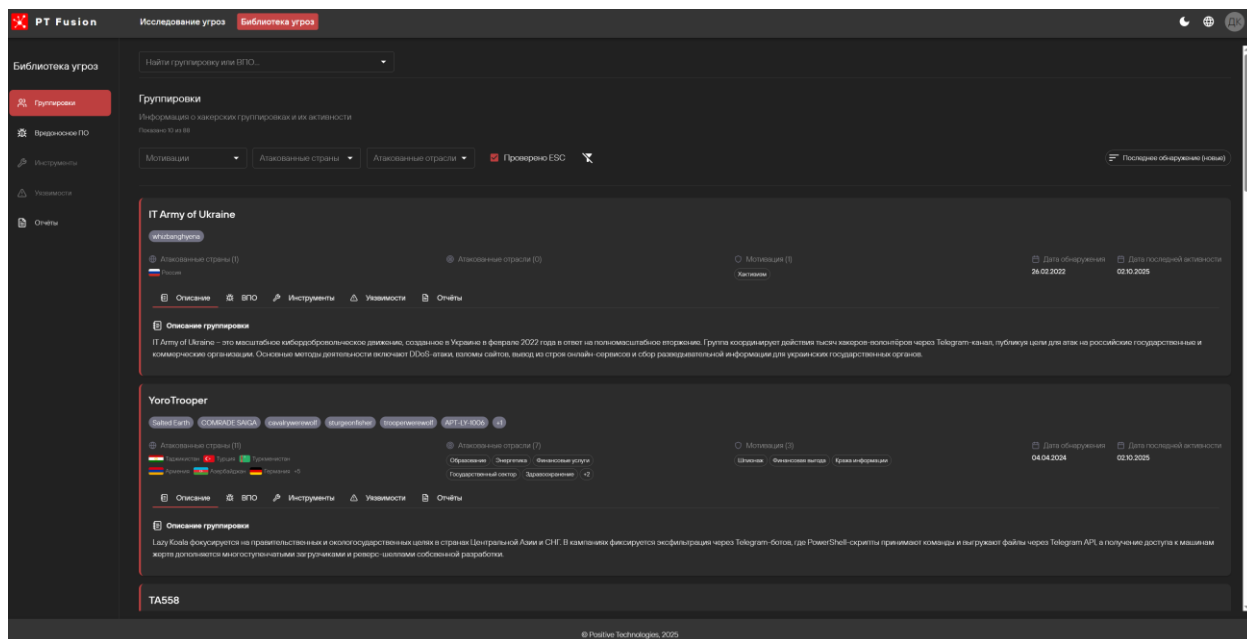


Рисунок 33. Главная страница раздела «Библиотека угроз»

В разделе «Библиотека угроз» представлено 5 подразделов:

- Группировки
- Вредоносное ПО
- Инструменты
- Уязвимости
- Отчеты

Подраздел «Группировки»

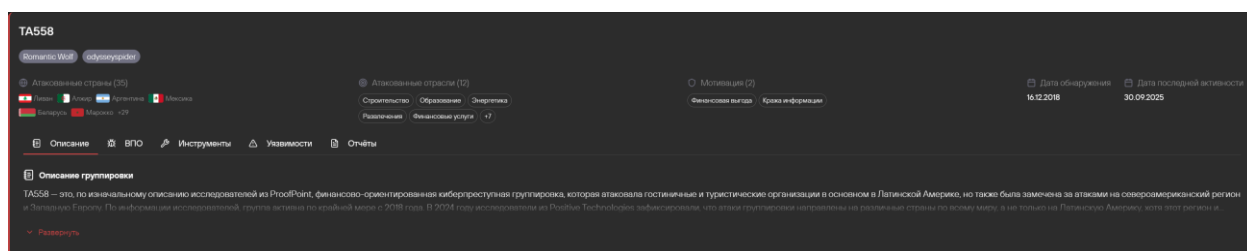


Рисунок 34. Быстрая карточка группировки

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

Название	Первое использование	Последнее использование
Agent Tesla	01.01.2014	29.08.2025
XWorm	01.01.2022	24.09.2025
Remcos	01.01.2016	24.08.2025

Рисунок 35. Связь с ВПО в быстрой карточке группировки

- Используемые инструменты

Название инструменты	Класс	Тип ОС
NirxSoft	-	-
AnyDesk	RemoteAccess	-
DefenderControl	-	-

Рисунок 36. Связь с инструментами в быстрой карточке группировки

- Используемые уязвимости

Идентификатор	Платформа	Дата публикации
CVE-2017-11882	Windows	15.11.2017
CVE-2017-11882	Windows	15.11.2017

Рисунок 37. Связь с уязвимостями в быстрой карточке группировки

– Связанные публичные отчеты о группировке

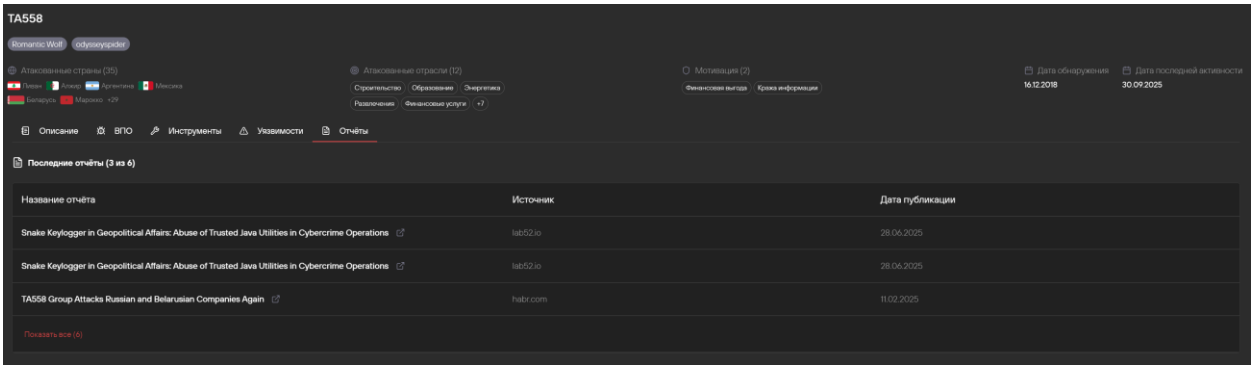


Рисунок 38. Связь с публичными отчетами в быстрой карточке группировки

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

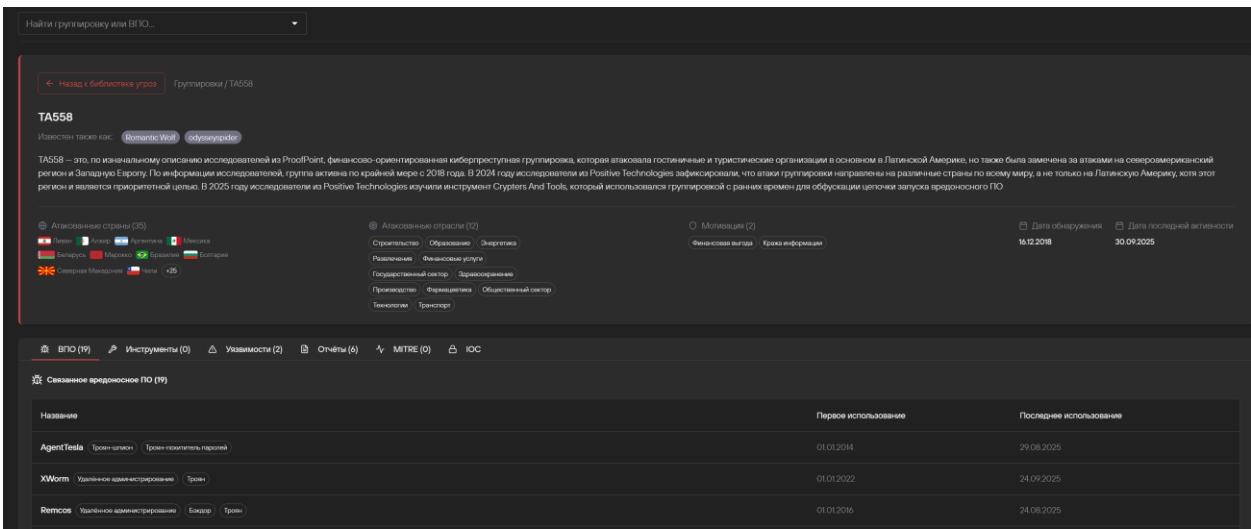


Рисунок 39. Основная карточка группировки

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.

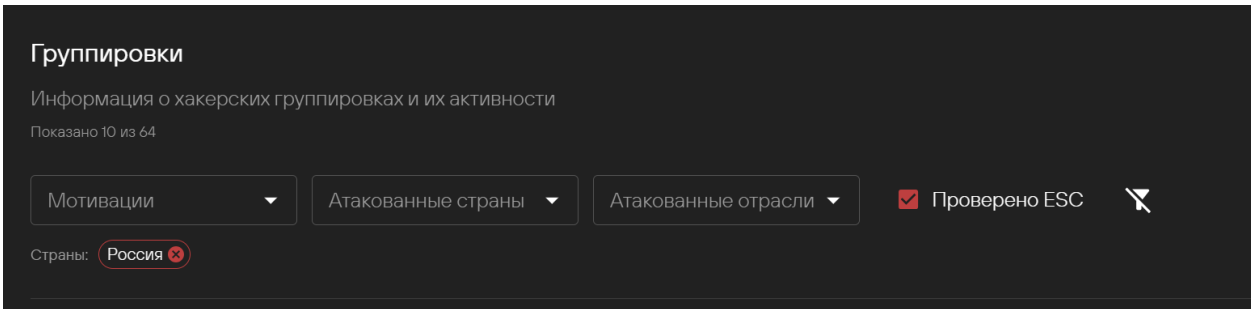


Рисунок 40. Фильтры для подраздела «Группировки»

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»

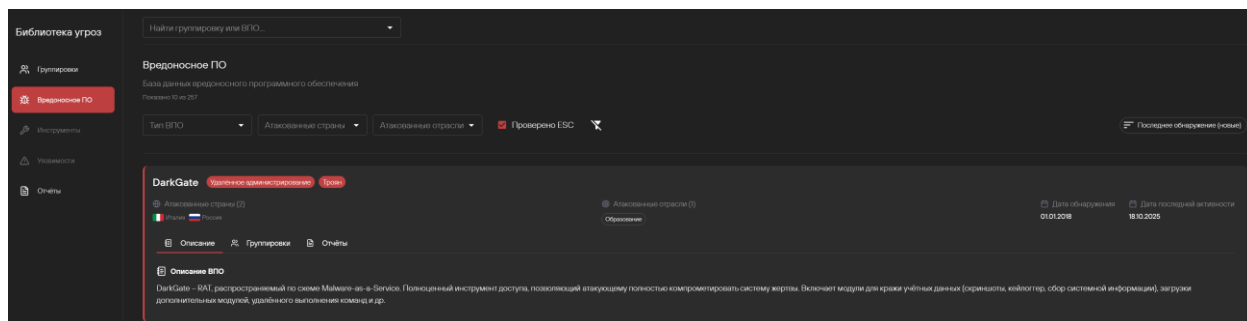


Рисунок 41. Быстрая карточка ВПО

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 ту же самую информацию плюс ТТР ВПО и индикаторы компрометации, которые можно скачать в формате CSV.

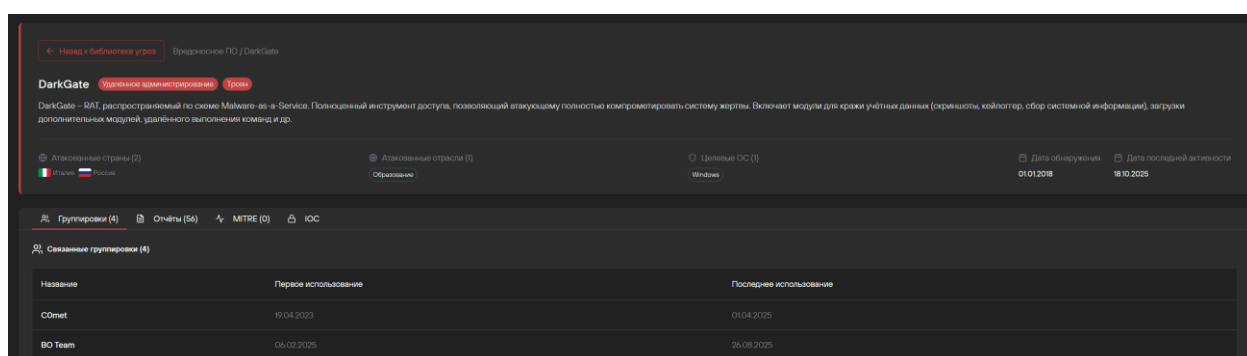


Рисунок 42. Основная карточка ВПО

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

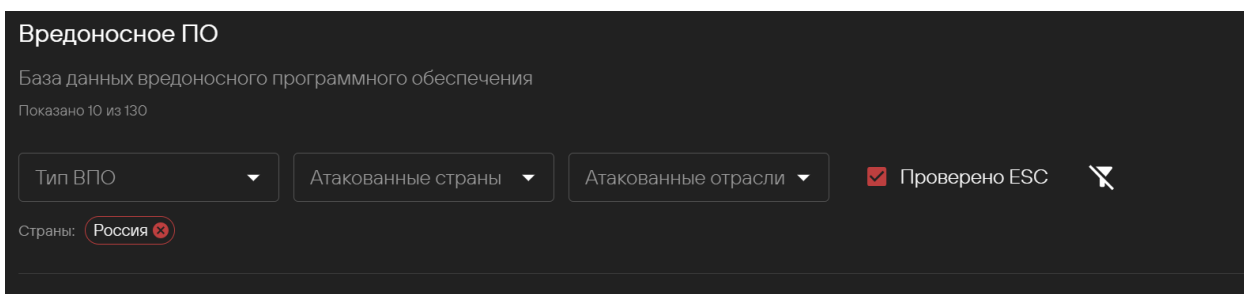


Рисунок 43. Фильтры для подраздела «ВПО»

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»

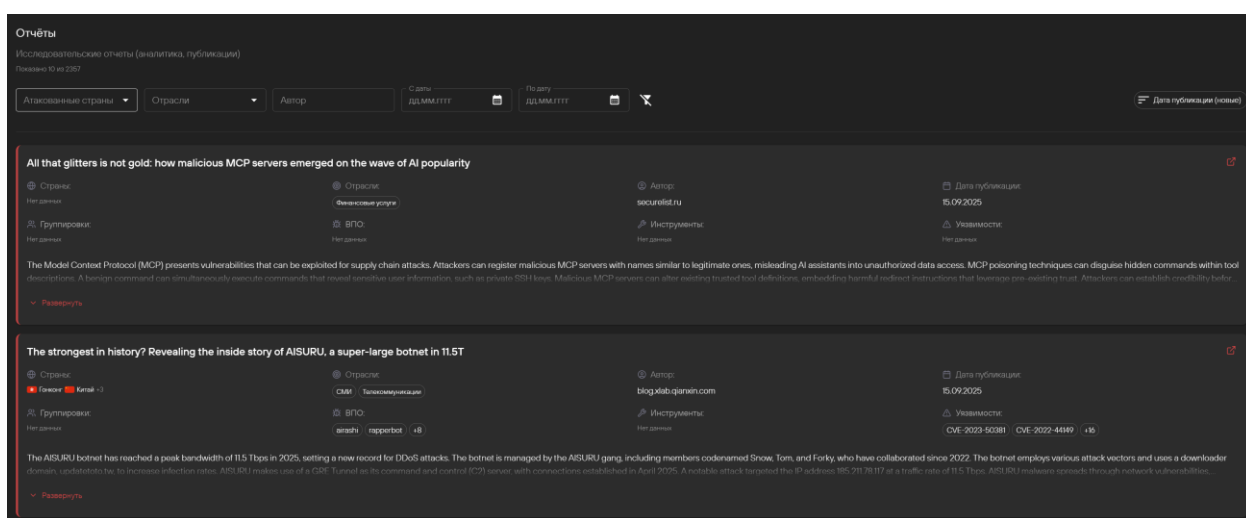


Рисунок 44. Быстрая карточка отчета

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 ту же самую информацию.

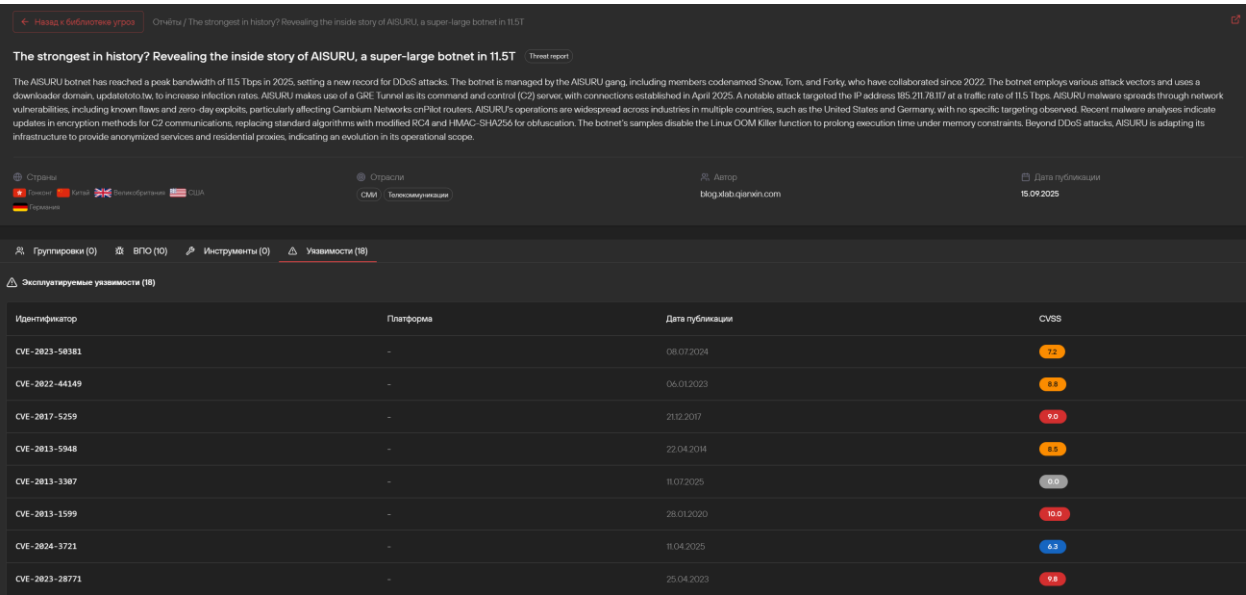


Рисунок 45. Основная карточка отчета

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

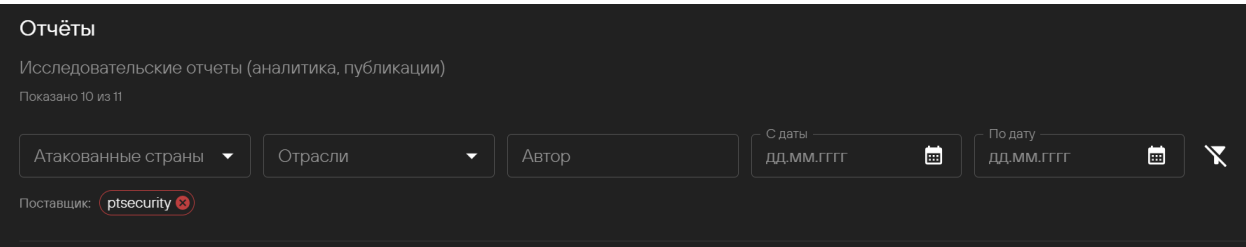


Рисунок 46. Фильтр в подразделе «Отчеты»

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.

The screenshot shows the 'Личный кабинет' (Personal Account) interface. On the left is a sidebar with 'Профиль' (Profile) selected. The main area is divided into three sections:

- Информация профиля** (Profile Information): Fields for 'Имя и фамилия' (Name and Surname) with value 'Smith ONE' and 'Email' with value 'smith1@corp.com'.
- Смена пароля** (Change Password): Fields for 'Старый пароль' (Old password), 'Новый пароль' (New password), and 'Подтверждение нового пароля' (New password confirmation), each with a visibility toggle. A 'СМЕНИТЬ ПАРОЛЬ' (Change Password) button is at the bottom.
- Настройки пользователя** (User Settings): A dropdown for 'Источник IP-информации' (IP information source) set to 'РФ' (Russia), and a toggle for 'Почтовые уведомления' (Email notifications) which is currently off.

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.

The screenshot shows the 'Личный кабинет' (Personal Account) interface with the 'Подписка' (Subscription) tab selected. The main area displays:

- Информация о подписке** (Subscription Information): A summary card showing 'Дата выдачи' (Issue date) 03.10.2025 11:50, 'Истекает' (Expires) 02.11.2025 11:50, 'Осталось' (Remaining) 27, 'Максимум пользователей' (Maximum users) ∞, and 'Доступ к API' (API access) Да (Yes). A progress bar for 'Срок действия (прогресс)' (Validity period (progress)) is shown.
- Квоты** (Quotas): A table showing quotas for 'Portal' and 'API'.
- Управление пользователями** (User Management): A table listing users and their roles.

Resource	Макс. запросов/период (Max requests/period)	Окно (Window)	Следующий сброс квоты (Next quota reset)	До сброса (Until reset)
Portal	∞	1 дн.	07.10.2025 11:50	18 часов
API	5 000	1 дн.	07.10.2025 11:50	18 часов

Email	Имя (Name)	Роль (Role)	Приглашение (Invitation)	Последний вход (Last login)	Добавлен (Added)
smith1@corp.com	Smith ONE	Менеджер (Manager)	✓ Принято (Accepted)	—	03.10.2025 11:50
smith2@corp.com	Smith TWO	Менеджер (Manager)	✓ Принято (Accepted)	—	03.10.2025 11:50

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.