

Программное обеспечение, выполняющее функции информационного справочника о территориальном распределении IP-адресов «Jet Geo IP»

Общее описание системы

Содержание

1 Назначение программного обеспечения	3
1.1 Вид деятельности, для автоматизации которых предназначено программное обеспечение.....	3
1.2 Перечень объектов автоматизации, на которых используется GeoIP	3
1.3 Перечень функций, реализуемых GeoIP.....	3
2 Описание GeoIP.....	5
2.1 Сведения необходимые для обеспечения эксплуатации GeoIP	5
2.2 Структура GeoIP и назначение ее частей.....	5
2.2.1 Структура GeoIP в рамках основных функций.....	5
2.2.2 Структура GeoIP в рамках дополнительных функций	8
2.3 Описание функционирования GeoIP и его частей	10
2.3.1 Рабочий (штатный) режим	10
2.3.2 Режим ТО	10
3 Описание взаимосвязей со сторонним ПО	12
4 Описание GeoIP	13
4.1 Структура GeoIP и назначение их частей.....	13
4.2 Описание функционирования GeoIP и их частей	14
4.2.1 Скачиватели GeoIP и Tor/Proху	14
4.2.2 Графический пользовательский интерфейс	19
4.2.3 Планировщик	35
4.2.4 Сценарии GeoIP.....	37
4.3 Сведения об подсистемах и их частях, необходимых для обеспечения их функционирования.....	40
4.3.1 Журналы событий.....	40
4.3.2 Конфигурационные файлы	41
4.3.3 Интернет-источники	42
4.3.4 База данных	43
4.3.5 Программные интерфейсы	45
4.3.6 Состав технических и программных средств	57
5 Перечень принятых сокращений.....	59
6 Перечень терминов.....	60

1 Назначение программного обеспечения

1.1 Вид деятельности, для автоматизации которых предназначено программное обеспечение

Программное обеспечение «Jet Geo IP» (далее – GeoIP) предназначено для использования в качестве информационного справочника о территориальном распределении IP-адресов.

1.2 Перечень объектов автоматизации, на которых используется GeoIP

GeoIP автоматизирует деятельность пользователей, связанную со следующими функциями:

- обновление справочника о географическом местоположении IP-адресов на основе данных интернет-источников;
- обогащение справочника о географическом местоположении IP-адресов дополнительными сведениями, включая:
- признаки принадлежности IP-адресов Tor/Proxy-узлам – на основе данных интернет-источников;
- признаки принадлежности IP-адресов и доменных имен контролируемым ресурсам субъектов – на основе данных стороннего ПО;
- получение выписки по IP-адресу;
- предоставление данных о географическом местоположении IP-адресов;
- предоставление в графическом пользовательском интерфейсе отчетности на основе данных справочника о географическом местоположении IP-адресов, включая историю изменений;
- хранение истории о территориальном распределении IP-адресов сети Интернет и владеющих ими субъектах, а также о принадлежности IP-адресов контролируемым субъектам и удаление устаревшей информации по истечению срока хранения;
- получение регистрационных сведений и abuse-контактов IP-адреса;
- получение сведений о доменных именах IP-адреса;
- получение репутационного показателя IP-адреса;
- просмотр и внесение комментариев к IP-адресу;
- массовый анализ IP-адресов;
- поиск организации по доменному имени.

1.3 Перечень функций, реализуемых GeoIP

GeoIP реализует следующие функции:

- формирование справочника о территориальном распределении IP-адресов сети Интернет и об их владельцах на основе данных интернет-источников (далее – GeoIP-данные);

- обогащение данных справочника признаками принадлежности IP-адресов к Tor и Proxu сетевым узлам на основе данных интернет-источников (далее – Tor/Proxu-данные);
- обогащение данных справочника признаками принадлежности IP-адресов и доменных имен контролируемым ресурсам (далее – контролируемые ресурсы);
- получение выписки по IP-адресу;
- ведение истории изменения:
 - географического местоположения IP-адресов,
 - владельцев IP-адресов;
- принадлежности IP-адресов и доменных имен к контролируемым ресурсам;
- принадлежности IP-адресов к Tor и Proxu узлам;
- предоставление данных справочника;
- формирование отчетности по хранящимся в GeoIP объектам и их характеристикам, отображение данных в графическом пользовательском интерфейсе;
- получение регистрационных сведений и abuse-контактов IP-адреса;
- получение сведений о доменных именах IP-адреса;
- получение репутационного показателя IP-адреса;
- получение и внесения комментариев к IP-адресу;
- массовый анализ IP-адресов;
- поиск организации по доменному имени.

2 Описание GeoIP

2.1 Сведения необходимые для обеспечения эксплуатации GeoIP

Функции GeoIP условно разделены на две группы:

- группа функций информационного справочника о территориальном распределении IP-адресов сети Интернет (далее – основные функции);
- группа функций, которые относятся к получению дополнительных сведений об IP-адресах, доменных именах и субъектах (далее – дополнительные функции).
- GeoIP в рамках основных функций предназначено:
- для формирования справочника о территориальном распределении IP-адресов сети Интернет и об их владельцах на основе данных интернет-источников (далее – GeoIP-данные);
- обогащения данных справочника признаками принадлежности IP-адресов к Tor и Proxu сетевым узлам на основе данных интернет-источников (далее – Tor/Proxu-данные);
- обогащения данных справочника признаками принадлежности IP-адресов и доменных имен контролируемым ресурсам (далее – контролируемые ресурсы);
- ведения истории изменения:
 - географического местоположения IP-адресов;
 - владельцев IP-адресов;
 - принадлежности IP-адресов и доменных имен к контролируемым ресурсам;
 - принадлежности IP-адресов к Tor и Proxu узлам;
- предоставления данных справочника стороннему ПО;
- формирования отчетности о хранящихся в GeoIP объектах и их характеристикам, отображения данных в графическом пользовательском интерфейсе.

GeoIP в рамках дополнительных функций предназначена:

- для получения регистрационных сведений и abuse-контактов IP-адреса (см. раздел 4.2.2.4);
- получения сведений о доменных именах IP-адреса (см. раздел 4.2.2.5);
- получения репутационного показателя IP-адреса (см. раздел 4.2.2.6);
- просмотра и внесения комментариев к IP-адресу (см. раздел 4.2.2.7);
- выполнения массового анализа IP-адресов (см. раздел 4.2.2.8);
- поиска организации по доменному имени (см. раздел 4.2.2.9);
- получения выписки по IP-адресу (см. раздел 4.2.2.3).

2.2 Структура GeoIP и назначение ее частей

2.2.1 Структура GeoIP в рамках основных функций

На рисунке 1 приведена логическая схема GeoIP в рамках основных функций.

и доменного имени контролируемому ресурсу по запросу взаимодействующего ПО.

- 3) **Скачиватель GeolP** – программа, которая скачивает GeolP-данные из интернет-источника, преобразовывает и выгружает их в GeolP-файлы. Если в источнике GeolP-данных присутствует информация об автономных системах, то данные скачиваются и сохраняются в отдельных ASN-файлах.
- 4) **Скачиватель Tor/Proху** – программа, которая скачивает список Tor/Proху из интернет-источника, преобразовывает и выгружает его в Tor/Proху-файлы.
- 5) **Загрузчик GeolP** – модуль GeolP, который преобразовывает и загружает данные GeolP-файлов в базу данных модуля Справочник GeolP. Если в источнике GeolP-данных присутствовала информация об автономных системах, то соответствующие этому источнику ASN-файлы загружаются в базу данных модуля «Справочник GeolP».
- 6) **Загрузчик Tor/Proху** – модуль GeolP, который преобразовывает и загружает Tor/Proху-файлы в базу данных модуля «Справочник GeolP».
- 7) **Планировщик** – модуль GeolP, который запускает по расписанию следующие процессы:
 - скачивание GeolP-данных и Tor/Proху-данных;
 - перенос скачанных данных;
 - загрузка GeolP-файлов и Tor/Proху-файлов в базу модуля «Справочник GeolP»;
 - удаление устаревших данных из базы данных модуля «Справочник GeolP» и устаревших скачанных файлов;
 - запрос данных контролируемых ресурсов.
- 8) **Справочник GeolP** – модуль GeolP, который отвечает за следующие процессы:
 - хранение в БД:
 - GeolP, Tor/Proху и ASN-данных;
 - данных контролируемых ресурсов;
 - предоставление следующих данных посредством API:
 - GeolP, Tor/Proху и ASN-данных;
 - признаков принадлежности IP-адресов и доменных имен контролируемым ресурсам;
 - получение данных контролируемых ресурсов от стороннего ПО;
 - удаление устаревших данных модуля «Справочник GeolP».
- 9) **ГПИ** – модуль графического пользовательского интерфейса, который получает данные из модуля «Справочник GeolP» посредством API GeolP. В рамках основных функций модуль предназначен для отображения следующей информации об IP-адресе:
 - географическое местоположение с указанием источников данных;
 - данные владельца;
 - признак принадлежности к контролируемому ресурсу;
 - признак принадлежности к Tor и Proху-узлам;

- история изменения географического местоположения;
- история изменения владельца;
- история изменения признака принадлежности к Tor и Proxy-узлам;
- история загрузки файлов обновлений в базу данных модуля «Справочник GeolP»;
- идентификаторы и наименования организаций, которым принадлежат контролируемые ресурсы.

В рамках основных функций к входным данным GeolP относятся:

- GeolP-данные интернет-источников;
- ASN-данные интернет-источников;
- Tor/Proxy-данные интернет-источников;
- IP-адреса контролируемых ресурсов;
- доменные имена контролируемых ресурсов;
- идентификаторы и имена организаций контролируемых ресурсов.

В рамках основных функций к выходным данным относятся:

- данные географического местоположения IP-адреса;
- дополнительные сведения, которые включают в себя признаки принадлежности IP-адресов Tor/Proxy-узлам;
- сведения о принадлежности IP-адресов и доменных имен контролируемым ресурсам;
- сведения о владельцах IP-адресов на основании информации об автономных системах;
- исторические данные IP-адресов с информацией об изменениях географического местоположения, владельца, принадлежности к Tor/Proxy-узлам и к контролируемым ресурсам;
- данные журнала событий загрузки информации в базу данных модуля «Справочник GeolP»;
- данные журнала событий API GeolP.

2.2.2 Структура GeolP в рамках дополнительных функций

На рисунке 2 приведена логическая схема GeolP в рамках дополнительных функций.

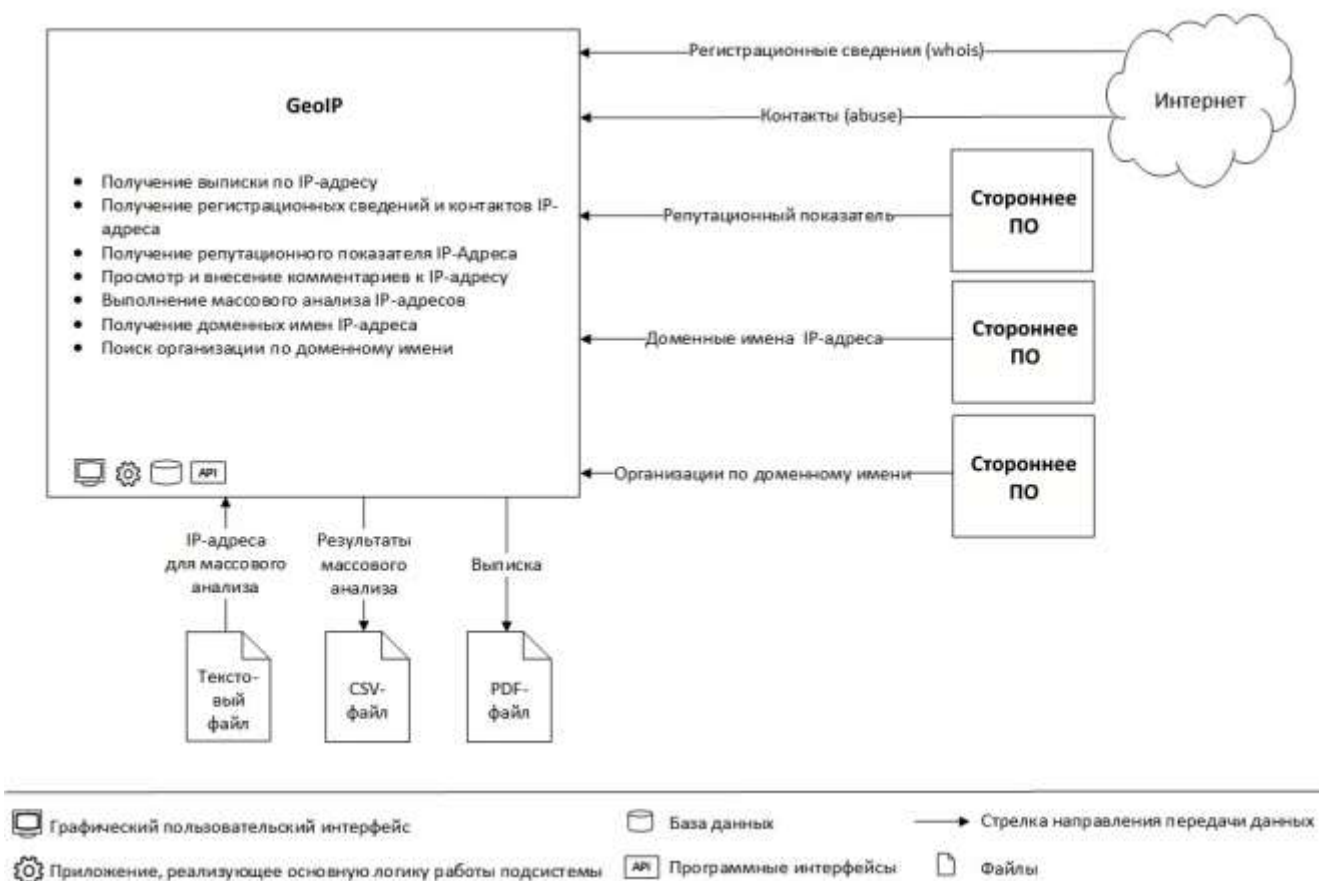


Рисунок 2 – Логическая схема GeoIP в рамках дополнительных функций

На схеме представлены:

- 10) **GeoIP**, которая включает в себя дополнительные функции.
- 11) **Интернет** – источник регистрационных сведений (whois) и контактов (abuse) IP-адресов, которые запрашивает GeoIP.
- 12) **Стороннее ПО** – у которого GeoIP запрашивает репутационный показатель IP-адресов, из которого GeoIP получает доменные имена IP-адресов, по запросу передает GeoIP названия организаций, которым принадлежит указанное в запросе доменное имя.
- 13) **Текстовый файл** – содержит списки IP-адресов, которые загружает GeoIP для дальнейшего массового анализа.
- 14) **CSV-файл** – содержит выгрузку результатов массового анализа IP-адресов.
- 15) **PDF-файл** – содержит выгрузку выписки по IP-адресу.

В рамках дополнительных функций к ГПИ подсистемы относятся:

- форма получения регистрационных сведений и контактов IP-адреса;
- форма получения сведений о доменных именах IP-адреса;
- форма получения репутационного показателя IP-адреса;
- форма просмотра и внесения комментариев к IP-адресу;
- форма выполнения массового анализа IP-адресов;

- форма поиска организации по доменному имени.

К дополнительным функциям подсистемы также относится функция получения выписки по IP-адресу, которая реализована в форме поиска IP-адреса (см. раздел 4.2.2.3).

В рамках дополнительных функций к входным данным GeoIP относятся:

- регистрационные сведения (whois);
- контакты (abuse);
- репутационный показатель;
- доменные имена IP-адреса;
- идентификаторы и имена организаций контролируемых ресурсов;
- текстовый файл со списком IP-адресов для массового анализа.

В рамках дополнительных функций к выходным данным GeoIP относятся:

- CSV-файл с результатами массового анализа;
- PDF-файл, содержащий выписку по IP-адресу.

2.3 Описание функционирования GeoIP и его частей

Для GeoIP предусмотрены следующие режимы функционирования:

- рабочий (штатный) режим;
- режим технического обслуживания (далее – ТО).

2.3.1 Рабочий (штатный) режим

В рабочем (штатном) режиме GeoIP обеспечивает:

- решение функциональных задач;
- работу пользователей.

Режим функционирования GeoIP – 24 часа в сутки 7 дней в неделю (24x7).

Полноценное функционирование GeoIP обеспечивается только в рабочем (штатном) режиме.

2.3.2 Режим ТО

В режим ТО GeoIP переводится по следующим причинам:

- проведение планового технического обслуживания;
- нарушение работоспособности отдельных компонентов;
- нарушение функционирования поддерживающей инфраструктуры – общесистемных сервисов, сетей электропитания, каналов связи и т. п.;
- несанкционированный доступ к ресурсам.

В режиме ТО выполняются:

- разбор конфликтных ситуаций;
- модернизация элементов;
- техническое обслуживание;
- замена батарей ИБП;

- диагностирование инцидентов или проблем, связанных либо со сбоями или авариями в работе компонентов GeoIP, либо с попытками НСД к ее ресурсам;
- оперативное противодействие попыткам НСД;
- восстановление при необходимости программно-аппаратной конфигурации компонентов;
- расследование причин НСД или аварии и определение источника инцидента или проблемы.

Установка, замена, первоначальное конфигурирование и дополнительная настройка компонентов GeoIP проводятся в соответствии с эксплуатационной документацией компаний-производителей этих средств в режимах, обеспечивающих сервисное обслуживание программно-аппаратных средств и предусматривающих временный останов или отдельных ее компонентов.

Реагирование на попытки НСД и аварийные ситуации включает принятие контрмер, восстановление информации, выработку и проведение профилактических мероприятий.

После первичной диагностики и определения причин НСД или аварии GeoIP проводится тестирования ее функционирования и при успешном прохождении всех тестов и проверок переводится в рабочий (штатный) режим функционирования.

При успешном выполнении сервисных работ (прохождении всех тестов и проверок функционирования) GeoIP переводится в рабочий (штатный) режим.

3 Описание взаимосвязей со сторонним ПО

GeoIP взаимодействует со сторонним ПО:

- для получения идентификатора и наименования организации в рамках поиска организации по доменному имени;
- для получения репутационного показателя IP-адреса;
- для получения доменных имен IP-адреса.

4 Описание GeoIP

4.1 Структура GeoIP и назначение их частей

GeoIP в рамках выполнения основных функций состоит из следующих модулей:

- 1) **Скачиватель GeoIP** – программа, которая скачивает данные географического местоположения IP-адресов (GeoIP-данные) из интернет-источников и сохраняет эти данные в файлы стандартизованного вида (GeoIP-файлы). Для каждого интернет-источника разрабатывается собственная программа-скачиватель. Если в интернет-источнике присутствует информация об автономных системах (ASN-данные), то программа скачивает ASN-данные и сохраняет их в файлы стандартизованного вида (ASN-файлы). Перечень источников GeoIP-данных приведен в разделе 4.3.3. Описание скачивателей приведено в разделе 4.2.1.

Примечание. Скачиватели GeoIP не входят в состав GeoIP и разрабатываются отдельно.

- 2) **Скачиватель Tor/Proху** – программа, которая скачивает данные принадлежности IP-адресов Tor-узлам и Proху-узлам (Tor/Proху-данные) из интернет-источников и сохраняет эти данные в файлы стандартизованного вида (Tor/Proху-файлы). Для каждого интернет-источника разрабатывается собственная программа-скачиватель. Перечень источников Tor/Proху-данных приведен в разделе 4.3.3. Описание скачивателей приведено в разделе 4.2.1.

Примечание. Скачиватели Tor/Proху не входят в состав GeoIP и разрабатываются отдельно.

- 3) **Загрузчик GeoIP** – модуль, который загружает GeoIP и ASN-файлы в базу данных. Описание загрузчиков приведено в разделе 4.2.1.1.
- 4) **Загрузчик Tor/Proху** – модуль, который загружает Tor/Proху-файлы в базу данных. Описание загрузчиков приведено в разделе 0.
- 5) **Справочник GeoIP** – модуль, который выполняет следующие функции:
 - получение данных IP-адресов и доменных имен, которые принадлежат контролируемым ресурсам субъектов (далее – контролируемые ресурсы);
 - хранение GeoIP, ASN и Tor/Proху-данных, данных IP-адресов и доменных имен, которые принадлежат контролируемым ресурсам;
 - предоставление GeoIP, ASN и Tor/Proху-данных стороннему ПО, а также модулю графического пользовательского интерфейса по запросу посредством программных интерфейсов (API).

Описание модуля «Справочник GeoIP» приведено в разделе 0.

- 6) **Графический пользовательский интерфейс (ГПИ)** – модуль, который предназначен для отображения данных модуля «Справочник GeoIP». Описание модуля приведено в разделе 4.2.2.
- 7) **Планировщик** – модуль, который предназначен для запуска процессов по расписанию. Описание модуля приведено в разделе 4.2.3.

4.2 Описание функционирования GeoIP и их частей

4.2.1 Скачиватели GeoIP и Tor/Proxy

В GeoIP за получение данных из интернет-источников отвечают специальные программы-скачиватели. К их функциям относятся:

- скачивание из интернет-источников GeoIP, ASN и Tor/Proxy-данных;
- сохранение скачанных данных в файлы стандартизованного вида: GeoIP-файлы, ASN-файлы, Tor/Proxy-файлы.

Скачивание данных происходит по расписанию в соответствии с графиком обновления данных в интернет-источниках. Расписание настраивается с помощью модуля «Планировщик» (см. раздел 4.2.3.1). Данные, в которых фигурируют IP-адреса или блоки IP-адресов, сохраняются в отдельные файлы для версий IPv4 и IPv6.

Все виды создаваемых скачивателями файлов содержат в своем имени:

- имя источника данных;
- вид скачиваемых данных;
- версию IP-адресов, фигурирующих в файлах;
- дату и время создания файла.

Примечание. Имя источника данных должно быть указано в конфигурационном файле GeoIP (см. раздел 4.3.2).

Все создаваемые файлы скачиватели размещают в одном месте расположения.

Создаваемые файлы соответствуют следующим положениям:

- тип файла – CSV;
- расширение имени файла – csv;
- используются строки с заголовками;
- символ ограничитель строковых значений – двойная кавычка;
- символ разделитель – запятая;
- кодировка – UTF8.

Имя GeoIP-файла имеет структуру:

`<имя_источника>_geoipN_<дата_создания>.csv`

где:

- <имя_источника> – имя источника данных. Состоит из букв в любом регистре и цифр; длина не превышает 10 символов;
- geoipN – вид данных содержимого файла, где N – номер версии IP-адресов 4 или 6;
- <дата_создания> – дата и время создания файла с точностью до микросекунд.

GeoIP-файл содержит следующие поля (Таблица 1):

Таблица 1 – Поля GeoIP-файла

Поле	Описание	Обязательность
created_at	Дата и время обновления в интернет-источнике	Да
ip_first	Первый IP-адрес сети	Да

ip_last	Последний IP-адрес сети	Да
subnet	Подсеть	Да
country_code	Код страны в соответствии со стандартом ISO 3166-2. Наименование страны определяется с помощью справочника по коду страны и приводится на русском языке	Да
country_name	Наименование страны географического местоположения	Да
region_name	Наименование региона географического местоположения	Нет
city_name	Наименование города или населенного пункта географического местоположения	Нет
internet_service_provider_name	Наименование провайдера	Нет
is_anycast	Признак того, что IP-адреса относятся к корневому DNS-серверу. Возможные значения: - Y – относятся; - N – не относятся; - U – не определено	Да

Имя ASN-файла имеет структуру:

`<имя_источника>_asnN_<дата_создания>.csv`

где:

- `<имя_источника>` – имя источника данных. Состоит из букв в любом регистре и цифр; длина не превышает 10 символов;
- `asnN` – вид данных содержимого файла, где N – номер версии IP-адресов 4 или 6;
- `<дата_создания>` – дата и время создания файла с точностью до микросекунд.

ASN-файл содержит следующие поля (Таблица 2):

Таблица 2 – Поля ASN-файла

Поле	Описание	Обязательность
created_at	Дата и время обновления в интернет-источнике	Да
ip_first	Первый IP-адрес сети	Да
ip_last	Последний IP-адрес сети	Да
subnet	Подсеть	Да
asn	Номер автономной системы	Да
asn_info	Данные владельца автономной системы	Да

Имя Tor/Proxy-файла имеет структуру:

`<имя_источника>_tor|proxyN_<дата_создания>.csv`

где:

- <имя_источника> – имя источника данных. Состоит из букв в любом регистре и цифр; длина не превышает 10 символов;
- Tor|ProxyN – вид данных содержимого файла Tor или Proxy, где N – номер версии IP-адресов 4 или 6;
- <дата_создания> – дата и время создания файла с точностью до микросекунд.

Tor/Proxy-файл содержит следующие поля (Таблица 3):

Таблица 3 – Поля Tor/Proxy-файла

Поле	Описание	Обязательность
created_at	Дата и время обновления в интернет-источнике	Да
ip	IP-адрес	Да

Для GeoIP-файлов и ASN-файлов выполняются следующие действия:

- 1) Если в файле блок IP-адресов представлен в виде подсети в формате CIDR, то блок преобразовывается в диапазон IP-адресов, представленного первым и последним IP-адресом блока. Полученные значения сохраняются в поля ip_first и ip_last.
- 2) Если в файле блок IP-адресов представлен в виде диапазона IP-адресов, представленного значениями первого и последнего IP-адреса блока, то диапазон преобразовывается в подсеть в формате CIDR. Полученные значения сохраняются в поле subnet. Если нет возможности преобразовать диапазон IP-адресов в одну подсеть в формате CIDR, то одна запись файла разбивается на несколько таким образом, чтобы это стало возможным.

Настройка скачивателей выполняется с помощью конфигурационного файла (см. раздел 4.3.2).

Загрузчики GeoIP и Tor/Proxy

4.2.1.1 Формирование локальных копий, скачанных из интернет-источников данных

GeoIP загружает файлы из разных источников в базу данных модуля «Справочник GeoIP» с помощью модулей загрузчиков. Реализованы следующие виды:

- загрузчик GeoIP – для GeoIP и ASN-файлов;
- загрузчик Tor/Proxy – для Tor/Proxy-файлов.

Предусмотрены следующие места расположения файлов, с которыми работают загрузчики:

- исходная директория файлов, в которой размещаются файлы всех видов, прежде не загруженные в модуль «Справочник GeoIP»;
- директория для успешно загруженных файлов;
- директория для файлов, не загруженных в результате возникшей ошибки загрузки.

Перечисленные места расположения файлов указаны в конфигурационном файле GeoIP (см. раздел 4.3.2).

Загрузчики запускаются по расписанию с помощью модуля «Планировщик» (см. раздел 4.2.3.1). Периодичность запуска настраивается индивидуально для каждого вида загрузчика. Каждый загрузчик сканирует исходную директорию файлов и, если файлы его вида обнаружены, выполняет загрузку.

Загружаются только те файлы, для которых в конфигурационном файле GeoIP (см. раздел 4.3.2) указаны соответствующие имена интернет-источников.

Примечание. Имена источников содержатся в именах файлов (см. подробную информацию в разделе 4.2.1).

Файлы загружаются последовательно в порядке увеличения значений имен файлов.

В GeoIP реализована функция загрузки файла в базу данных модуля «Справочник GeoIP» отдельными порциями записей. Для этого размер порции должен быть указан в конфигурационном файле Подсистемы (см. раздел 4.3.2). Если в конфигурационном файле размер порции не указан или равен нулю, то разделение записей на порции не применяется.

Успешно загруженные файлы после загрузки приводятся к упакованному виду с помощью программы gzip. Имя упакованного файла:

`<имя_исходного_файла>.gz.`

После упаковки файл переносится из исходной директории в директорию для успешно загруженных файлов.

Файлы, которые не удалось загрузить в базу данных модуля «Справочник GeoIP» в результате возникшей ошибки, переносятся из исходной директории в директорию для не загруженных файлов.

Загрузчики сохраняют события загрузки в журнал (см. раздел 4.3.1).

Загрузчик завершает работу после того, как отработал все файлы соответствующего ему вида.

Загрузчик GeoIP переносит данные GeoIP и ASN-файлов в базу данных модуля «Справочник GeoIP» в таблицы geoipv4, geoipv6, asnipv4, asnipv6 (см. описание структуры таблиц в разделе 4.3.4).

Загрузчик Tor/Proху загружает данные Tor/Proху-файлов в базу данных модуля «Справочник GeoIP» в таблицы toripv4, toripv6, proхuipv4, proхuipv6 (см. описание структуры таблиц в разделе 4.3.4).

Поля файлов переносятся в одноименные поля соответствующих таблиц.

Для заполнения поля таблицы «Источник» имя источника берется из имени загружаемого файла. Все записи из файла сохраняются в таблицу независимо от того, менялись ли значения атрибутов этих новых записей относительно предыдущей загрузки.

4.2.1.2 Обеспечение возможности внесения дополнительных сведений о IP-адресе

В GeoIP используются следующие виды дополнительных сведений:

- признак принадлежности IP-адреса Tor-узлу;

- признак принадлежности IP-адреса Proxu-узлу.

GeoIp загружает Tor/Proxu-данные с помощью скачивателей из интернет-источников (см. раздел 4.2.1). Tor/Proxu-файлы помещаются в базу данных модуля «Справочник GeoIP» с помощью загрузчиков (см. раздел 0).

Дополнительные сведения хранятся в таблицах:

- Toripv4 и Toripv6 – для Tor-узлов;
- Proxuiipv4 и Proxuiipv6 – для Proxu-узлов.

Описание структуры таблиц приведено в разделе 4.3.4.

Справочник GeoIP

4.2.1.3 Хранение истории о территориальном распределении IP-адресов сети Интернет и владеющих ими субъектах, а также о принадлежности IP-адресов контролируемым субъектам

Модуль «Справочник GeoIP» хранит в своей БД:

- данные территориального распределения IP-адресов – в таблицах geoipv4 и geoipv6;
- данные владельцев IP-адресов, полученные на основе данных автономных систем, – в таблицах asnipv4 и asnipv6.

Данные помещаются в приведенные выше таблицы с помощью загрузчиков (см. раздел 0). В результате формируется история изменения территориального распределения IP-адресов.

Данные контролируемых ресурсов в части IP-адресов хранятся в таблицах supervisedipv4 и supervisedipv6 IPv6.

Данные контролируемых ресурсов в части доменных имен хранятся в таблице superviseddomain.

Данные контролируемых ресурсов попадают в таблицы базы данных модуля «Справочник GeoIP» в результате запроса соответствующей информации у стороннего ПО (см. раздел 4.2.1.5).

Описание структуры таблиц приведено в разделе 4.3.4.

4.2.1.4 Предоставление данных стороннему ПО

По запросу стороннего ПО, GeoIP посредством API предоставляет данные:

- наиболее вероятного географического местоположения IP-адреса, включая информацию о владельцах и признаки принадлежности IP-адреса контролируемым ресурсам и Tor/Proxu-узлам;
- расширенной информации о географическом местоположении IP-адреса, включая информацию из нескольких источников и в том числе о владельцах и признаках принадлежности IP-адреса контролируемым ресурсам и Tor/Proxu-узлам;
- истории изменения географического местоположения IP-адреса;
- принадлежности IP-адреса автономным системам (владельцы IP-адресов);

- принадлежности IP-адреса контролируемому ресурсу;
- принадлежности доменного имени контролируемому ресурсу;
- загрузки файлов обновлений.

Описание API модуля приведено в разделе 4.3.5.

4.2.1.5 Получение данных контролируемых ресурсов

GeoIP запрашивает и получает данные IP-адресов и доменных имен контролируемых ресурсов из стороннего ПО, в котором реализован соответствующий программный интерфейс (API).

В качестве входных данных в запросе используется дата и время последней загрузки в подсистему GeoIP данных контролируемых ресурсов.

В ответ на запрос стороннего ПО передает:

- список блоков IP-адресов или единичные IP-адреса версии IPv4;
- список блоков IP-адресов или единичные IP-адреса версии IPv6;
- список доменных имен;
- идентификаторы организаций, которым принадлежат IP-адреса и доменные имена.

Полученные списки содержат только новые и измененные данные, дата и время изменения информационных записей которых больше даты и времени, указанных в запросе.

Список блоков IP-адресов содержит следующие данные:

- дату и время фактического изменения статуса контроля: установления контроля над ресурсом или выведения из-под контроля;
- блок IP-адресов в формате CIDR;
- идентификаторы организаций, которым принадлежит блок IP-адресов;
- статус контроля: «Под контролем» или «Выведено из-под контроля».

Каждый одиночный IP-адрес преобразуется в блок в формате CIDR.

Список доменных имен содержит следующие данные:

- дату и время фактического изменения статуса контроля: установления контроля над ресурсом или выведения из-под контроля;
- доменное имя в формате FQDN;
- идентификаторы организаций, которым принадлежит доменное имя;
- статус контроля: «Под контролем» или «Выведено из-под контроля».

Полученные из стороннего ПО данные сохраняются в таблицы:

- supervisedipv4 и supervisedipv6 – для IP-адресов контролируемых ресурсов;
- superviseddomain – для доменных имен контролируемых ресурсов.

Структура таблиц приведена в разделе 4.3.4.

4.2.2 Графический пользовательский интерфейс

Графический пользовательский интерфейс GeoIP представляет собой веб-приложение, которое работает в среде браузера. Авторизация для работы с модулем не требуется.

ГПИ подсистемы состоит из следующих элементов:

- форма поиска IP-адресов;
- форма получения регистрационных сведений и контактов IP-адреса;
- форма получения сведений о доменных именах IP-адреса;
- форма получения репутационного показателя IP-адреса;
- форма просмотра и внесения комментариев к IP-адресу;
- форма выполнения массового анализа IP-адресов;
- форма поиска организации по доменному имени.

Для переключения между формами в ГПИ GeoIP предусмотрено меню «Выберите действие» (см. рисунок 3). Подробное описание меню приведено в разделе 4.2.2.1.

Заголовок формы представляет собой строку, которая состоит из (см. рисунок 3):

- левой части – логотип и название подсистемы;
- центральной части – название формы;
- правой части, в которой отображается:
 - IP-адрес для форм «Поиск IP-адреса», «Получение регистрационных сведений и контактов IP-адреса», «Получение доменных имен IP-адреса», «Получение репутационного показателя IP-адреса», «Просмотр и внесение комментариев к IP-адресу»;
 - имя файла для формы «Выполнение массового анализа»;
 - доменное имя для формы «Поиск организации по доменному имени».

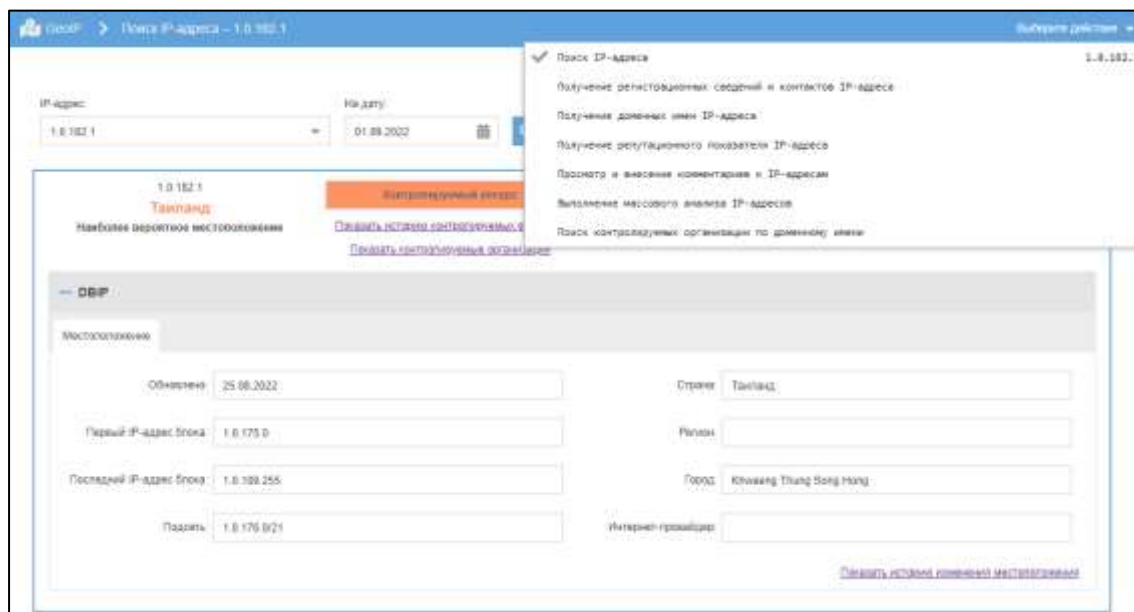


Рисунок 3 – Вид меню GeoIP

Правая часть заголовка формы заполнена, если пользователь запустил выполнение действия в форме. Например, если в форме поиска IP-адресов пользователь заполнил поля «IP-адрес», «На дату» и запустил поиск с помощью кнопки «Поиск» (см. рисунок 3), то в правой части заголовка отобразится введенный IP-адрес.

После запуска программы все формы находятся в исходном состоянии:

- отсутствуют сведения с результатами выполнения действий в форме;
- правая часть заголовка формы не заполнена.

В каждой форме предусмотрена кнопка «Очистить», при нажатии на которую форма возвращается в исходное состояние.

4.2.2.1 Меню

Для переключения между формами в ГПИ GeoIP предусмотрено меню «Выберите действие», которое состоит из пунктов:

- Поиск IP-адреса;
- Получение регистрационных сведений и контактов IP-адреса;
- Получение доменных имен IP-адреса;
- Получение репутационного показателя IP-адреса;
- Просмотр и внесение комментариев к IP-адресу;
- Выполнение массового анализа IP-адресов;
- Поиск организации по доменному имени.

Вид меню подсистемы приведен на рисунке 3.

Выбор пункта меню приводит к отображению соответствующей формы в открытой вкладке браузера. Выбор пункта меню при зажатой кнопке Ctrl (Windows, Linux) или кнопке Cmd (Mac) приводит к открытию формы в новой вкладке браузера. Выбранный пункт меню отмечен значком «галочка».

Название пункта меню состоит из двух частей:

- слева отображается название пункта меню;
- справа отображается:
 - IP-адрес для пунктов меню «Поиск IP-адреса», «Получение регистрационных сведений и контактов IP-адреса», «Получение доменных имен IP-адреса», «Получение репутационного показателя IP-адреса», «Просмотр и внесение комментариев к IP-адресу»;
 - имя файла для пункта меню «Выполнение массового анализа»;
 - доменное имя для пункта меню «Поиск организации по доменному имени».

Правая часть пункта меню не заполнена, если соответствующая форма находится в изначальном состоянии. Правая часть пункта меню заполняется, если пользователь запустил выполнение действия в соответствующей форме. Например, если в форме поиска IP-адресов пользователь заполнил поля «IP-адрес» и «На дату» (см. рисунок 3), то после нажатия кнопки «Поиск»:

- запускается поиск;
- в пункте меню «Поиск IP-адреса» справа отображается искомый IP-адрес;
- искомый IP-адрес также отображается в заголовке формы справа от названия формы.

4.2.2.2 Формирование отчетности по хранящимся объектам и их характеристикам

Отчетность в GeoIP формируется в форме поиска IP-адресов и концентрирует в себе основные функции. В этой форме предусмотрены:

- раздел ввода условий поиска и отображения найденных данных, которые включают в себя географическое местоположение IP-адреса и его владельцев, признаки принадлежности Tor/Proxy-узлам и контролируемым ресурсам;
- раздел истории изменения географического местоположения IP-адреса с таблицей, в которую включены записи обновлений данных географического местоположения IP-адреса;
- раздел истории смены владельцев IP-адреса с таблицей, в которую включены записи обновлений данных принадлежности IP-адреса автономной системе;
- раздел истории загрузки файлов обновлений с таблицей, в которую включены записи из журнала загрузки файлов обновлений;
- раздел истории изменения контролируемых ресурсов IP-адреса с таблицей, в которую включены записи изменений: ресурс помещен под контроль, ресурс выведен из-под контроля, сменилась организация контролируемого ресурса;
- раздел истории изменения признака принадлежности IP-адреса Tor/Proxy-узлам с таблицей, в которую включены записи обновлений тех дней, когда IP-адрес принадлежал Tor/Proxy-узлу;
- форма отображения наименований организаций контролируемых ресурсов.

Разделы формы поиска IP-адресов получают данные из базы данных модуля «Справочник GeoIP» посредством API (описание API приведено в разделе 4.3.5).

На рисунке 4 приведен вид раздела ввода условий поиска и отображения найденных данных, которые включают в себя географическое местоположение IP-адреса и его владельцев, признаки принадлежности Tor/Proxy-узлам и контролируемым ресурсам.

The screenshot displays the GeoIP search interface. At the top, there's a header bar with the GeoIP logo and navigation links. Below the header, a search bar contains the IP address '1.0.182.1' and a date '01.09.2022'. To the right of the search bar are buttons for 'Поиск', 'Выход', 'Справка', and a link to 'Показать историю загрузок файлов обновлений'. Below the search bar, there's a section for '1.0.182.1' with a 'Наиболее вероятное местоположение' (Most likely location) and a 'Владелец' (Owner) field. Below this, there are four tabs: 'Владелец', 'История изменений', 'История загрузки файлов обновлений', and 'История изменений IP-адреса'. The 'Владелец' tab is active, showing a table with columns for 'Местоположение' (Location), 'Обновлено' (Updated), 'Первый IP-адрес блока' (First IP address of the block), 'Последний IP-адрес блока' (Last IP address of the block), 'Подпись' (Signature), 'Страна' (Country), 'Регион' (Region), 'Таблица' (Table), and 'Интернет-провайдер' (Internet service provider). The table contains one row with the following data: 'Тайланд' (Thailand), '25.08.2022', '1.0.175.0', '1.0.180.255', '1.0.176.0/21', 'Тайланд', 'Bangkok', 'Thailand', and 'Thailand'. Below the table, there's a link to 'Показать историю изменений местоположения'.

Рисунок 4 – Раздел ввода условий поиска и отображения найденных данных

Раздел включает в себя:

- элементы ввода исходных данных для поиска;
- элементы основной информации, полученной в результате поиска географического местоположения IP-адреса, которые содержат данные наиболее вероятного местоположения;
- элементы представления развернутой информации, полученной в результате поиска, в виде единообразных блоков, которые содержат данные интернет-источников.

Основная информация результатов поиска представлена страной местонахождения и признаками принадлежности IP-адреса к контролируемому ресурсу и Tor/Proxy-узлам.

Развернутые данные местоположения представлены в ГПИ виде единообразных блоков, которые содержат данные каждого источника GeoIP-данных. Каждый блок представлен двумя вкладками:

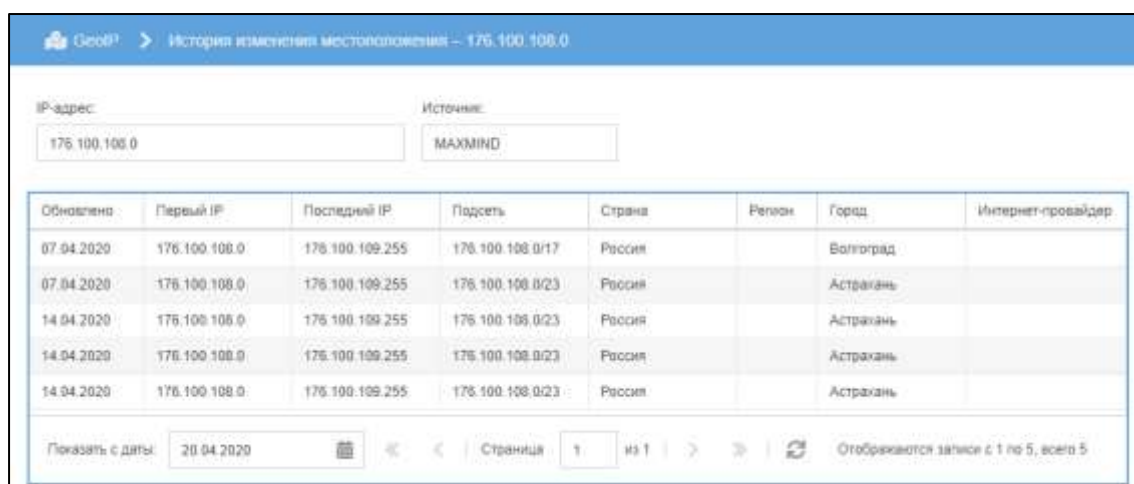
- местоположение IP-адреса;
- владельцы IP-адреса.

Кнопка «Поиск» предназначена для запуска поиска IP-адреса. Кнопка доступна, если заполнено поле «IP-адрес».

Кнопка «Выписка» предназначена для формирования выписки по IP-адресу. Кнопка доступна, если был выполнен поиск IP-адреса (см. раздел 4.2.2.3).

Кнопка «Очистить» предназначена для возвращения раздела ввода условий поиска и отображения найденных данных в исходное состояние. После нажатия кнопки очищаются поле «IP-адрес» и сведения результатов поиска географического местоположения IP-адреса.

На рисунке 5 приведен вид раздела истории изменения географического местоположения IP-адреса.



Обновлено	Первый IP	Последний IP	Подсеть	Страна	Регион	Город	Интернет-провайдер
07.04.2020	176.100.108.0	176.100.109.255	176.100.108.0/17	Россия		Волгоград	
07.04.2020	176.100.108.0	176.100.109.255	176.100.108.0/23	Россия		Астрахань	
14.04.2020	176.100.108.0	176.100.109.255	176.100.108.0/23	Россия		Астрахань	
14.04.2020	176.100.108.0	176.100.109.255	176.100.108.0/23	Россия		Астрахань	
14.04.2020	176.100.108.0	176.100.109.255	176.100.108.0/23	Россия		Астрахань	

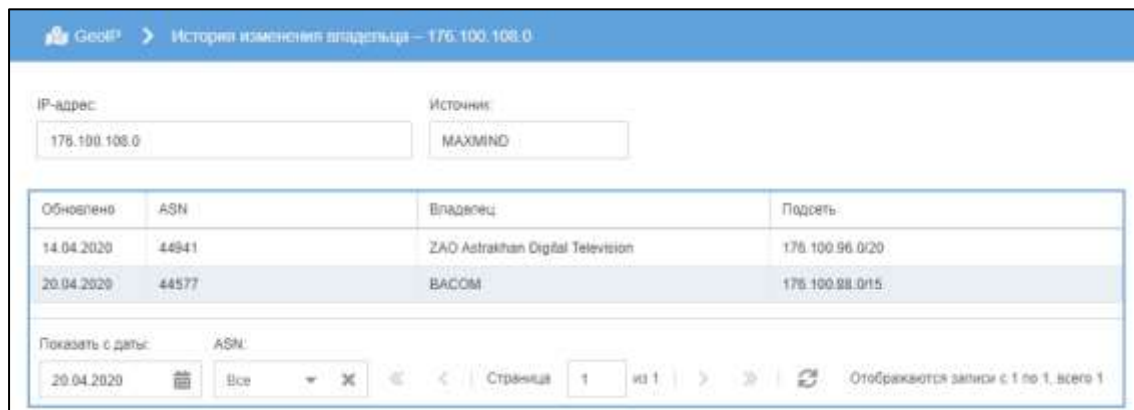
Рисунок 5 – Раздел истории изменения географического местоположения IP-адреса

Раздел открывается из формы поиска IP-адреса (см. рисунок 4) по нажатию гиперссылки «Показать историю изменения местоположения».

Запрос данных для формы исторических данных использует API предоставления исторических GeoIP-данных (см. раздел 4.3.5).

В разделе исторических данных представлена информация по искомому IP-адресу для одного источника GeoIP-данных. С помощью поля «Показать с даты» можно установить фильтр записей исторических данных.

На рисунке 6 приведен вид раздела истории смены владельцев IP-адреса.



GeoIP > История изменения владельца — 176.100.108.0

IP-адрес: 176.100.108.0 Источник: MAXMIND

Обновлено	ASN	Владелец	Подсеть
14.04.2020	44941	ZAO Astrakhan Digital Television	176.100.96.0/20
20.04.2020	44577	BACOM	176.100.98.0/15

Показать с даты: 20.04.2020 ASN: Все

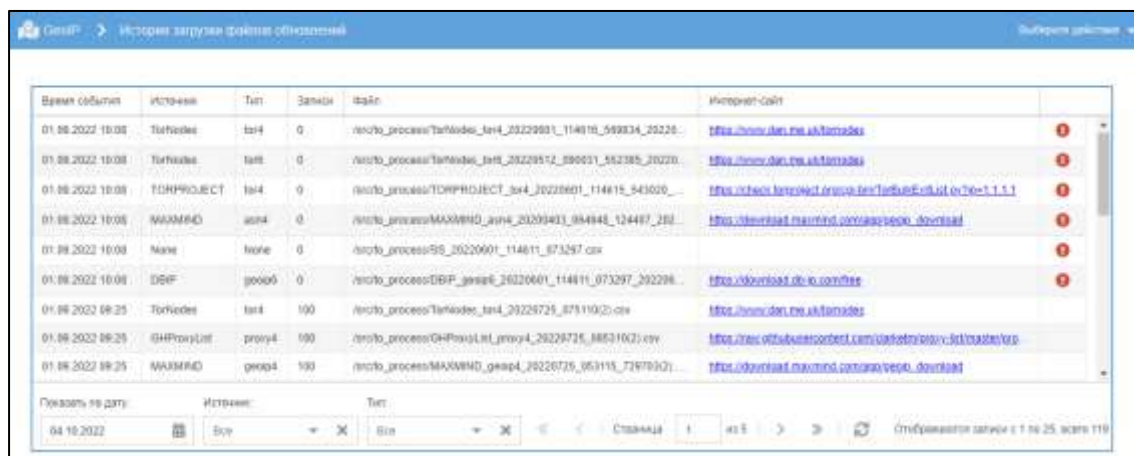
Страница 1 из 1 Отображаются записи с 1 по 1, всего 1

Рисунок 6 – Раздел истории смены владельцев IP-адреса

Раздел открывается из формы ввода условий поиска и отображения найденных данных» (см. рисунок 4) по нажатии гиперссылки «Показать историю изменения владельца».

В разделе исторических данных представлена информация по искомому IP-адресу для одного источника GeoIP-данных. С помощью полей «Показать с даты» и «ASN» можно устанавливать фильтр записей исторических данных.

На рисунке 7 приведен вид раздела истории загрузки файлов обновлений.



GeoIP > История загрузки файлов обновлений

Время события	Источник	Тип	Заголовок	Файл	Интернет-сайт
01.08.2022 10:08	TelNedex	tar4	0	/usr/local/process/TelNedex_tar4_20220801_114810_549334_20228...	https://www.tel-nex.ru/telnedex
01.08.2022 10:08	TelNedex	tar4	0	/usr/local/process/TelNedex_tar4_20220801_090031_552385_20228...	https://www.tel-nex.ru/telnedex
01.08.2022 10:08	TORPROJECT	tar4	0	/usr/local/process/TORPROJECT_tar4_20220801_114815_543000...	https://www.torproject.org/en/torproject-0.4.10-tor-1.1.1
01.08.2022 10:08	MAXMIND	asn4	0	/usr/local/process/MAXMIND_asn4_20220801_084848_124467_202...	https://download.maxmind.com/app/geoip_download
01.08.2022 10:08	MaxM	asn4	0	/usr/local/process/RS_20220801_114811_673297_20228...	https://download.maxmind.com/app/geoip_download
01.08.2022 10:08	DBF	geoip4	0	/usr/local/process/DBF_geoip4_20220801_114811_673297_20228...	https://download.maxmind.com/app/geoip_download
01.08.2022 08:25	TelNedex	tar4	100	/usr/local/process/TelNedex_tar4_20220725_07511020_075...	https://www.tel-nex.ru/telnedex
01.08.2022 08:25	GHFProxyList	proxy4	100	/usr/local/process/GHFProxyList_proxy4_20220725_08031020_075...	https://www.ghfproxylist.com/ghfproxylist-proxy4-tar4
01.08.2022 08:25	MAXMIND	geoip4	100	/usr/local/process/MAXMIND_geoip4_20220725_063115_72870320...	https://download.maxmind.com/app/geoip_download

Показать с даты: 04.10.2022 Источник: Все Тип: Все

Страница 1 из 5 Отображаются записи с 1 по 25, всего 119

Рисунок 7 – Раздел истории загрузки файлов обновлений

Раздел открывается из формы поиска IP-адреса (см. рисунок 4) с помощью кнопки «Показать историю загрузки файлов обновлений».

В разделе исторических данных представлена информация из журнала событий Подсистемы (см. раздел 4.3.1). С помощью полей «Показать с даты», «Источник» и «Тип» можно устанавливать фильтр записей исторических данных.

На рисунке 8 приведен вид раздела истории изменения контролируемых ресурсов IP-адреса.

Раздел открывается из формы поиска IP-адреса (см. рисунок 4) с помощью гиперссылки «Показать историю ресурсов».

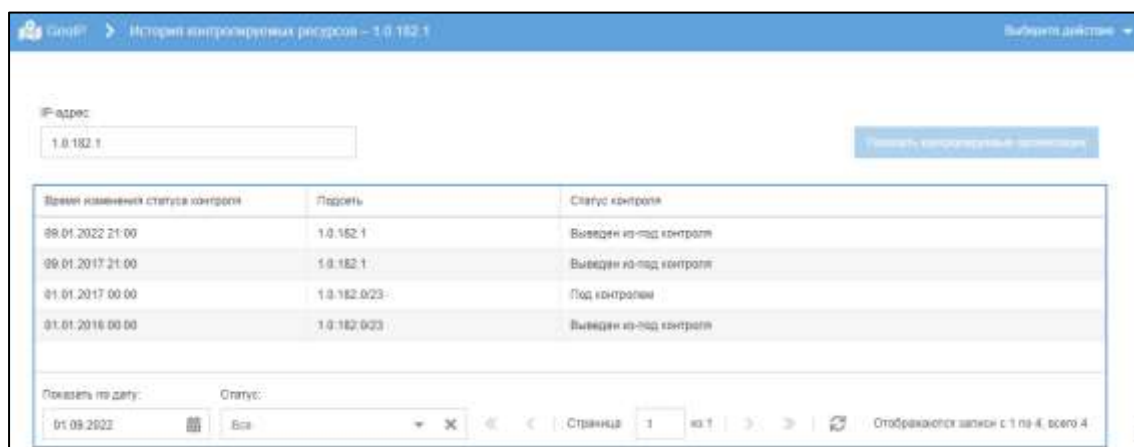


Рисунок 8 – Раздел истории изменения контролируемых ресурсов IP-адреса

Раздел предназначен для отображения изменения принадлежности IP-адреса контролируемому ресурсу. Из этой формы можно открыть форму отображения наименований организаций контролируемых ресурсов (см. рисунок 10).

С помощью полей «Показать с даты» и «Статус» можно устанавливать фильтр записей исторических данных.

На рисунке 9 приведен пример раздела истории изменения признака принадлежности IP-адреса Tor/Proxy-узлам.

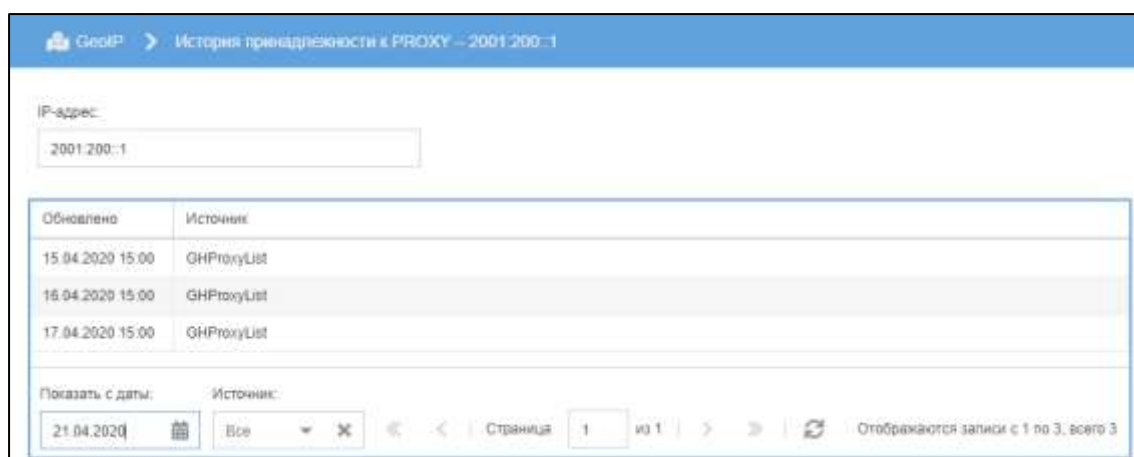


Рисунок 9 – Раздел истории изменения признака принадлежности IP-адреса Tor/Proxy-узлам

Раздел открывается из формы поиска IP-адреса (см. рисунок 4) с помощью гиперссылок «Показать историю Tor» и «Показать историю Proxy».

Этот раздел позволяет анализировать историю принадлежности IP-адреса Tor-узлам и Proxy-узлам.

С помощью полей «Показать с даты» и «Источник» можно устанавливать фильтр записей исторических данных.

На рисунке 10 приведен пример формы отображения наименований организаций контролируемых ресурсов.

Рисунок 10 – Форма отображения наименований организаций контролируемых ресурсов

Форма открывается в модальном окне из двух разделов формы поиска IP-адреса:

- раздела ввода условий поиска и отображения найденных данных с помощью гиперссылки «Показать организации»;
- раздела истории изменения контролируемых ресурсов IP-адреса с помощью кнопки «Показать организации».

Во время открытия формы GeoIP отправляет запрос стороннему ПО. В запросе указан список идентификаторов организаций, которым принадлежит IP-адрес. В ответ на запрос стороннее ПО возвращает массив организаций, каждый элемент которого состоит из идентификатора и наименования организации. После закрытия модального окна наименование организации на компьютере пользователя и на сервере GeoIP не сохраняется.

4.2.2.3 Получение выписки по IP-адресу

В форме поиска IP-адреса реализована возможность получения выписки по IP-адресу (рисунок 11).

Рисунок 11 – Форма поиска IP-адреса

Сценарий работы пользователя в форме поиска IP-адреса:

- 1) Пользователь заполняет поля «IP-адрес», «На дату» и нажимает кнопку «Поиск».
- 2) Подсистема выполняет поиск IP-адреса.
- 3) Пользователь нажимает кнопку «Выписка», которая доступна, только если искомый IP-адрес был найден.

В модальном окне появляется форма выбора разделов выписки (см. рисунок 12).

- 4) Пользователь использует флажки для включения/исключения разделов в выписке. При нажатии кнопки «Получить выписку» подсистема на основе сведений найденного IP-адреса формирует файл выписки в формате PDF и выгружает его.

Пользователь на этапе выбора разделов выписки может отказаться от формирования выписки, нажав кнопку «Отменить».

Рисунок 12 – Форма выбора разделов выписки

Выписка включает в себя:

- заголовок выписки;
- раздел сведений об IP-адресе;
- раздел сведений о наиболее вероятном местоположении IP-адреса;
- раздел сведений о владельцах IP-адреса;
- раздел сведений о принадлежности к TOR/PROXY узлам;
- раздел сведений о принадлежности к контролируемому ресурсу.

Пример выписки приведен на рисунке 13.

Выписка по IP-адресу на 01.09.2022

1. Сведения об IP-адресе

Искомый IP-адрес: 1.0.182.1

Первый IP-адрес блока: 1.0.175.0

Последний IP-адрес блока: 1.0.189.255

Подсеть: 1.0.176.0/21

2. Сведения о наиболее вероятном месторасположении IP-адреса

Страна: Таиланд

Регион: Не определен

Город: Khwaeng Thung Song Hong

Интернет-провайдер: Не определен

3. Сведения о владельцах IP-адреса

ASN	Владелец	Подсеть
-----	----------	---------

4. Сведения о принадлежности IP-адреса к TPR/PROXY узлам

Является звеном TOR-сети: Нет

Является анонимным PROXY: Нет

5. Сведения о принадлежности IP-адреса к контролируемому ресурсу

Является контролируемым ресурсом: Да

Рисунок 13 – Пример выписки по IP-адресу

4.2.2.4 Получение регистрационных сведений и контактов IP-адреса

Подсистема получает регистрационные сведения с помощью unix-утилиты whois.

Получение abuse-контактов выполняется путем извлечения сведений из региональных сетевых информационных центров.

Для получения регистрационных сведений и abuse-контактов в GeoIP предусмотрена форма получения регистрационных сведений и контактов IP-адреса (рисунок 14), которая

открывается после выбора пункта меню «Получение регистрационных сведений и контактов IP-адреса».

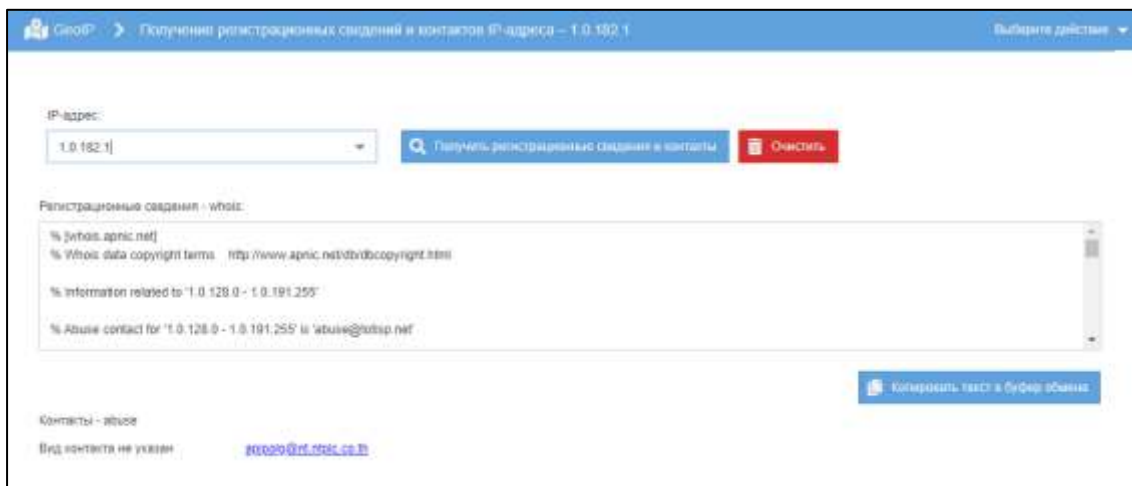


Рисунок 14 – Форма получения регистрационных сведений и контактов IP-адреса

Сценарий работы пользователя в форме получения регистрационных сведений и контактов IP-адреса:

- 1) Пользователь заполняет поле «IP-адрес» и запускает получение регистрационных сведений и abuse-контактов – нажимает кнопку «Получить регистрационные сведения и контакты».

Автоматически заполняются разделы формы «Регистрационные сведения – whois» и «Контакты – abuse». В случае отсутствия сведений разделы заполняются текстом: «Сведения не удалось получить или они отсутствуют».

В форме предусмотрена кнопка «Копировать текст в буфер обмена». При нажатии кнопки, сведения, приведенные в разделе «Регистрационные сведения – whois», копируются в буфер обмена.

Раздел «Контакты – abuse» содержит название вида email и email-адрес в виде гиперссылки, при нажатии на которую запускается клиентская часть программы электронной почты в режиме создания нового письма, в адресате которого указан выбранный email-адрес.

При отсутствии в разделе «Контакты – abuse» вида контакта, поле заполняется текстом: «Вид контакта не указан».

- 2) Пользователь нажимает кнопку «Очистить».

Форма получения регистрационных сведений и контактов IP-адреса возвращается в исходное состояние: очищаются от сведений поле «IP-адрес» и разделы формы «Регистрационные сведения – whois» и «Контакты – abuse».

4.2.2.5 Получение доменных имен IP-адреса

Подсистема получает сведения о доменных именах, делегированных IP-адресу, путем извлечения сведений с помощью WEB API из стороннего ПО.

Для получения доменных имен IP-адреса предусмотрена одноименная форма (рисунок 15), которая открывается после выбора пункта меню «Получение доменных имен IP-адреса».

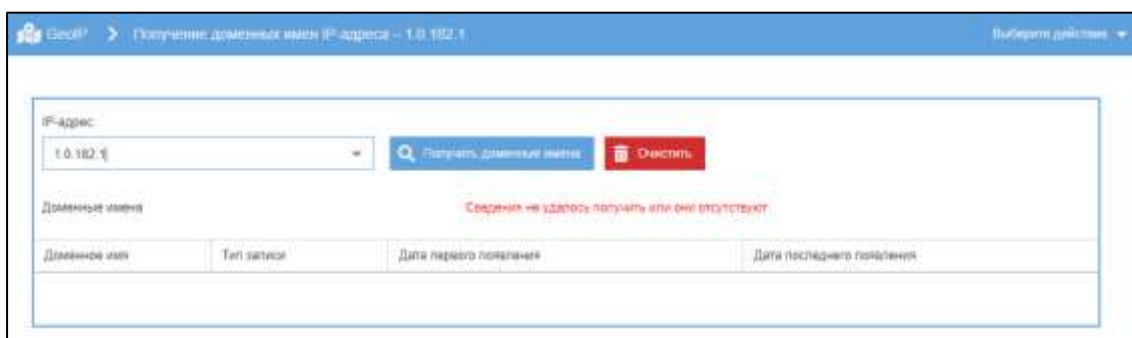


Рисунок 15 – Форма получения доменных имен IP-адреса

Сценарий работы пользователя в форме получения доменных имен IP-адреса:

- 1) Пользователь заполняет поле «IP-адрес» и запускает получение доменных имен – нажимает кнопку «Получить доменные имена».
Заполняется таблица «Доменные имена». При отсутствии сведений над таблицей появляется текст: «Сведения не удалось получить или они отсутствуют».
- 2) Пользователь нажимает кнопку «Очистить».
Форма получения доменных имен IP-адреса возвращается в исходное состояние: очищаются от сведений поле «IP-адрес» и таблица с доменными именами.

4.2.2.6 Получение репутационного показателя IP-адреса

Подсистема получает репутационный показатель IP-адреса путем извлечения сведений с помощью WEB API из стороннего ПО.

Для получения доменных имен IP-адреса предусмотрена одноименная форма (рисунок 16), которая открывается после выбора пункта меню «Получение доменных имен IP-адреса».

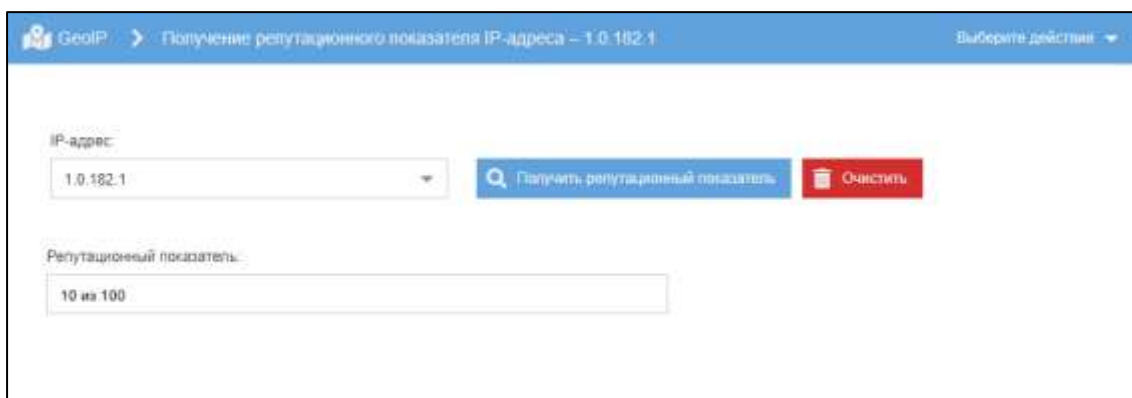


Рисунок 16 – Форма получения репутационного показателя IP-адреса

Сценарий работы пользователя в форме получения репутационного показателя IP-адреса:

- 1) Пользователь заполняет поле «IP-адрес» и запускает получение репутационного показателя – нажимает кнопку «Получить репутационный показатель». Заполняется поле формы «Репутационный показатель». При отсутствии сведений поле заполняется текстом: «Сведения не удалось получить или они отсутствуют».
- 2) Пользователь нажимает кнопку «Очистить». Форма получения доменных имен IP-адреса возвращается в исходное состояние: очищаются от сведений поля «IP-адрес», «Репутационный показатель».

4.2.2.7 Просмотр и внесение комментариев к IP-адресу в GeoIP

Для просмотра и внесения комментариев к IP-адресу в подсистеме предусмотрена одноименная форма (рисунок 17), которая открывается после выбора пункта меню «Просмотр и внесение комментариев к IP-адресу».

Комментарий	Время внесения	Автор	Контроль IP-адреса
Контроль IP-адреса проведен до 01.10.2022	22.07.2022 14:51	2001:200:1	01.10.2022
IP-адрес поставлен на контроль группы поддержки	22.07.2022 14:50	2001:200:1	

Рисунок 17 – Форма просмотра и внесения комментариев к IP-адресу

Сценарий работы пользователя в форме просмотра и внесения комментариев к IP-адресу:

- 1) Для просмотра сведений о ранее внесенных комментариях к IP-адресу пользователь заполняет поле «IP-адрес» и нажимает кнопку «Просмотр комментариев». В форме отображаются комментарии к указанному IP-адресу (см. рисунок 17). Записи в табличном списке комментариев следуют в порядке уменьшения времени внесения. Справа от табличного списка расположено текстовое поле для отображения комментария из выделенной строки.
- 2) Для внесения комментария к IP-адресу пользователь заполняет поле «IP-адрес» и нажимает кнопку «Внесение комментария». В форме отображаются комментарии к указанному IP-адресу. Поверх формы открывается окно внесения комментария (рисунок 18).
- 3) Пользователь вносит комментарий и закрывает окно внесения комментария:
 - с помощью кнопки «Сохранить», подтверждая сохранение комментария;
 - с помощью кнопки «Отменить», отказываясь от сохранения комментария.

Текстовое поле для ввода комментария допускает внесение текста размером до 5 000 символов.

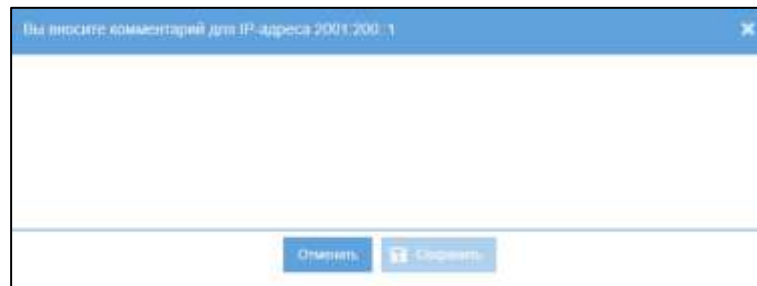


Рисунок 18 – Окно внесения комментария к IP-адресу

- 4) Пользователь нажимает кнопку «Очистить».

Форма просмотра и внесения комментариев к IP-адресу возвращается в исходное состояние: очищаются от сведений поле «IP-адрес» и табличный список с комментариями.

Для хранения комментариев к IP-адресам в базе данных подсистемы предусмотрена таблица comments (см. раздел 4.3.4).

4.2.2.8 Выполнение массового анализа IP-адресов

Для выполнения массового анализа IP-адресов предназначена одноименная форма (рисунок 19), которая открывается после выбора пункта меню «Выполнение массового анализа IP-адресов».

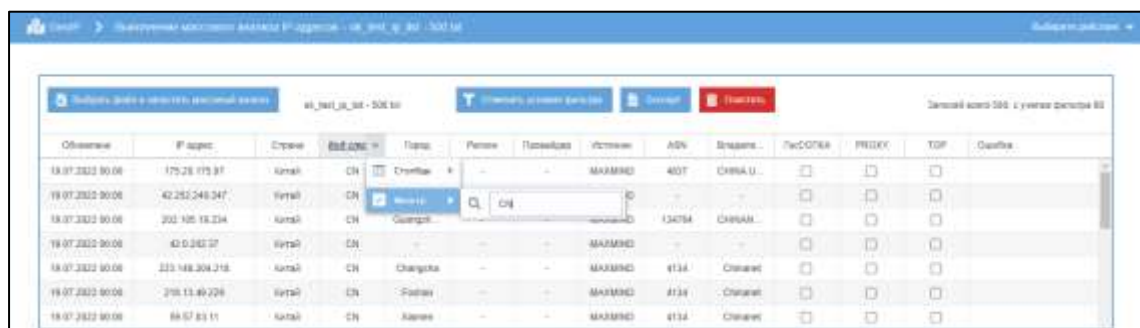


Рисунок 19 – Форма выполнения массового анализа IP-адресов

Сценарий работы пользователя в форме выполнения массового анализа IP-адресов:

- 1) Пользователь нажимает кнопку «Выбрать файл и запустить массовый анализ». Открывается программа выбора файла, например, проводник при использовании операционной системы Windows.
- 2) Пользователь выбирает файл с перечнем IP-адресов. Запускается выполнение массового анализа IP-адресов. Имя выбранного файла отображается справа от кнопки «Выбрать файл и запустить массовый анализ».

Массовый анализ IP-адресов представляет собой процесс сбора данных об IP-адресах, приведенных в файле с перечнем IP-адресов, хранящихся в БД подсистемы:

- сведения о наиболее вероятном местоположении IP-адресов на время выполнения анализа, включая страну, регион, город, дату последнего обновления данных о местоположении IP-адреса, имя интернет-источника данных о местоположении IP-адреса;
- наименование Интернет-провайдера IP-адреса;
- номер и имя владельца автономной системы IP-адреса (выбираются сведения с максимальным временем обновления);
- признак принадлежности IP-адреса к контролируемым ресурсам на время выполнения анализа;
- признак вхождения IP-адреса в перечень известных анонимных прокси-серверов на время выполнения анализа;
- признак хождения IP-адреса в перечень известных узлов сети TOR на время выполнения анализа.

Все приведенные выше сведения представлены в таблице «Результаты массового анализа» (рисунок 19). Таблица результатов анализа также содержит колонку «Ошибка», которая заполняется текстом «Неверный IP-адрес», если IP-адрес не соответствует формату IPv4 или IPv6.

При отсутствии в GeoIP некоторых сведений, соответствующие колонки в таблице «Результаты массового анализа» заполняются прочерками.

Подсистема обеспечивает возможность выполнения анализа до 50 000 IP-адресов. Файл с перечнем IP-адресов представляет собой текстовый файл в кодировке UTF-8, в котором каждый IP-адрес следует с новой строки.

Перед запуском анализа GeoIP проверяет, что в файле присутствует хотя бы один IP-адрес. Если проверка не пройдена, то:

- в форме массового анализа IP-адресов отображается сообщение «Возникла ошибка загрузки перечня IP-адресов. Проверьте файл» (см. рисунок 19);
- анализ не выполняется.

Порядок следования IP-адресов в таблице «Результаты массового анализа» такое же, как в файле с перечнем IP-адресов.

В форме выполнения массового анализа IP-адресов предусмотрена возможность экспорта результатов анализа в CSV-файл. Пользователь нажимает кнопку «Экспорт» после чего формируется файл с результатами анализа. Созданный CSV-файл результатов анализа автоматически скачивается на компьютер пользователя средствами браузера.

Параметры CSV-файла результатов анализа:

- расширение имени файла – csv;
- строка с заголовками колонок – используется заголовки таблицы «Результаты массового анализа»;

- символ ограничителя строковых значений – двойная кавычка;
- символ экранирования \ на случай, когда в поле присутствуют двойные кавычки;
- символ разделитель – запятая;
- Кодировка – UTF8;
- имя файла – geoip_analysis_result_<метка_времени>.
- Метка времени представлена в формате YYYYMMDDhhmmsszzz, где
- YYYY – год;
- MM – месяц;
- DD – день;
- hh – часы;
- mm – минуты;
- ss – секунды;
- zzz – миллисекунды.

Состав и порядок следования записей, а также состав, порядок следования и названия колонок CSV-файла результатов анализа, соответствуют аналогичным характеристикам таблицы «Результаты массового анализа».

3) Пользователь нажимает кнопку «Очистить».

Форма выполнения массового анализа IP-адресов возвращается в исходное состояние: очищаются от сведений таблица «Результаты массового анализа», имя выбранного файла со списком IP-адресов.

Также в форме выполнения массового анализа IP-адресов предусмотрена возможность фильтровать записи в таблице по значениям любой колонки. Для сброса условий фильтра по всем колонкам предусмотрена кнопка «Отменить условия фильтра».

4.2.2.9 Поиск организаций по доменному имени

Подсистема осуществляет поиск организаций по доменному имени с помощью API стороннего ПО.

Для выполнения поиска организаций по доменному имени предусмотрена одноименная форма (рисунок 20), которая открывается после выбора пункта меню «Поиск организации по доменному имени».

Идентификатор	Наименование
c24e9c5d-aa25-49e0-b4f5-41c788e@cb3d	АО "Металлоконструкции"

Рисунок 20 – Форма поиска организации по доменному имени

Сценарий работы пользователя в форме поиска организации по доменному имени:

- 1) Пользователь заполняет поле «Доменное имя» и нажимает кнопку «Поиск».
После этого GeolP:
 - a) Выполняет поиск введенного доменного имени в базе данных подсистемы в таблице superviseddomain в поле fqdn. Поиск выполняется среди записей, у которых значение поля is_supervised равно true. Поиск выполняется с учетом сценария определения совпадения доменных имен, реализованного в действующей версии GeolP.
 - б) Если записи не найдены, то завершает поиск, а таблицу со списком организаций не заполняет.
 - в) Если записи найдены, то отправляет запрос в стороннее ПО. В запросе к API указывается список идентификаторов организаций, которые расположены в поле company_id найденных записей таблицы superviseddomain.

В ответ на запрос стороннее ПО возвращает массив организаций, каждый элемент которого состоит из идентификатора и наименования организации.

Полученный массив организаций отображается в таблице со списком организаций.

- 2) Пользователь нажимает кнопку «Очистить».
Форма поиска организаций по доменному имени возвращается в исходное состояние: очищаются от сведений таблица со списком организаций, поле «Доменное имя».

4.2.3 Планировщик

4.2.3.1 Запуск процессов в GeolP

За запуск процессов отвечает модуль «Планировщик», который реализован с использованием системной программы cron.

С помощью этого модуля настраиваются:

- 1) Расписание запуска каждой программы-скачивателя (подробнее о скачивателях описано в разделе 4.2.1). Периодичность скачивания должна соответствовать дням и периодам обновления данных в интернет-источниках, но не может быть чаще одного раза в день.
- 2) Расписание запуска процедуры переноса файлов (подробнее о переносе файлов описано в разделе 4.2.3.2). По умолчанию запуск переноса файлов выполняется каждые 10 минут.
- 3) Расписание запуска загрузчиков (подробнее о загрузчиках описано в разделе 0). По умолчанию запуск выполняется каждые 10 минут.
- 4) Расписание запуска запроса контролируемых ресурсов (о получении данных контролируемых ресурсов см. в разделе 4.2.1.5). По умолчанию запуск выполняется каждый час.

- 5) Запуск удаления устаревших данных (подробнее об удалении устаревших данных описано в разделе 4.2.3.3). По умолчанию запуск выполняется каждое воскресенье в 1:00.

4.2.3.2 Перенос файлов

В GeolP реализован перенос файлов, созданных скачивателями, в место, где располагаются исходные файлы для загрузчиков.

Месторасположения файлов указано в конфигурационном файле GeolP (см. раздел 4.3.2).

Целевое месторасположение перенесенных файлов указано в конфигурационном файле GeolP (см. раздел 4.3.2).

Процедура переноса файлов запускается по расписанию с помощью модуля «Планировщик» (см. 4.2.3.1). Файлы переносятся последовательно в порядке увеличения значения имени файла (см. подробно об именах файлов в разделе 4.2.1). Если файл перенесен успешно, то в он удаляется.

Для переноса файлов используется SFTP-протокол. Перенос файлов фиксируется в журнале событий (см. в разделе 4.3.1). Процедура переноса завершается после отработки всех файлов.

4.2.3.3 Удаление устаревших данных

В Подсистеме реализованы механизмы удаления:

- устаревших данных из базы данных модуля «Справочник GeolP»;
- устаревших файлов.

К удаляемым данным и файлам применяется один срок хранения, по истечении которого устаревшие данные и файлы автоматически удаляются, и одно время запуска удаления устаревших данных и файлов.

С помощью конфигурационного файла GeolP настраивается срок хранения данных, который исчисляется в днях (см. раздел 4.3.2).

С помощью модуля «Планировщик» настраивается периодичность и время запуска удаления устаревших данных. Периодичность удаления соответствует условиям секционирования таблиц базы данных модуля «Справочник GeolP».

В GeolP предусмотрено удаление устаревших данных:

- GeolP-данных из таблиц `geoipv4` и `geoipv6`;
- данных принадлежности IP-адресов Tor-узлам из таблиц `Toripv4` и `Toripv6`;
- данных принадлежности IP-адресов Proxy-узлам из таблиц `Proxypv4` и `Proxypv6`;
- ASN-данных из таблиц `asnipv4` и `asnipv6`;
- данных журнала событий из таблицы `event_log`.

Удалению подлежат записи из перечисленных таблиц базы данных модуля «Справочник GeolP», у которых разница между сегодняшней датой и датой в поле «Дата и время обновления» больше срока хранения. Информация о таблицах базы данных приведена в разделе 4.3.4.

GeoIP удаляет успешно загруженные в базу данных модуля «Справочник GeoIP» файлы следующих видов:

- GeoIP-файлы;
- ASN-файлы;
- Tor/Proxy-файлы.

Файлы, у которых разница между сегодняшней датой и датой создания файлов, указанной в имени файлов, больше срока хранения, подлежат удалению. Местоположение файлов настроено в конфигурационном файле подсистемы (см. раздел 4.3.2).

4.2.4 Сценарии GeoIP

В подсистеме реализованы сценарии:

- вычисления наиболее вероятного местоположения IP-адреса;
- определения, является ли IP-адрес Tor/Proxy-узлом;
- поиска контролируемого ресурса по доменному имени.

4.2.4.1 Сценарий определения наиболее вероятного географического местоположения IP-адреса

Сценарий определяет процессы и методики для формирования заключения о наиболее вероятном географическом местоположении сетевого ресурса по присвоенному ему IP-адресу.

Сценарий задействует:

- рейтинги, заранее назначенные каждому интернет-источнику GeoIP-данных;
- принадлежность IP-адреса стране.

Настройка рейтинга источников GeoIP-данных выполняется исходя из экспертной оценки с помощью конфигурационного файла (см. раздел 4.3.2). В конфигурационном файле каждому источнику GeoIP-данных назначен рейтинг, который представляет собой целочисленное значение и обозначает уровень доверия к источнику: большее значение рейтинга указывает на большее доверие.

В качестве входных параметров сценарий использует:

- IP-адрес;
- дату и время, на которое запрашиваются GeoIP-данные для IP-адреса.

В качестве выходных данных сценарий использует запись из таблицы geoiprv4 или geoiprv6 (см. раздел 4.3.4).

При запросе данных из таблиц записи выбираются по следующим условиям, где дата и время обновления:

- меньше или равны дате и времени запроса и
- больше или равны дате и времени, вычисленных по формуле **В-Д**, где:
 - **В** – дата и время, указанное в запросе;
 - **Д** – диапазон времени в днях, указанный в конфигурационном файле (см. раздел 4.3.2).

Значение **Д** используется для уменьшения времени запроса данных. **Д** не должно быть меньше максимального периода обновления GeolP-данных в используемых интернет-источниках.

Если в разных источниках для IP-адреса указаны разные страны местоположения, то GeolP суммирует рейтинги источников по группам для каждой страны и выбирает один источник с максимальным рейтингом, который попадает в группу с максимальным суммарным рейтингом.

В таблице 4 приведено подробное описание сценария.

Таблица 4 – Сценарий определения наиболее вероятного географического местоположения IP-адреса

№	Шаг сценария
1.	Выполняется запрос GeolP-данных с применением входных параметров сценария. Ожидаемый ответ – записи данных из таблицы geoip_v4 или geoip_v6 актуальные на указанное в запросе дату и время, по одной на каждый источник GeolP-данных, в котором был найден запрашиваемый адрес
2.	Выполняется проверка: были ли найдены GeolP-данные? Если да, то переход к следующему шагу. Если нет, то: Формируются выходные параметры сценария в виде пустой записи GeolP-данных. Сценарий завершает работу
3.	Выполняется группировка полученных записей по стране. По каждой группе суммируются рейтинги источников
4.	Определяется группа с максимальным суммарным рейтингом
5.	Выполняется проверка: группа с максимальным суммарным рейтингом единственная? Если да, то: 1) Формируются выходные параметры сценария в виде записи из группы с максимальным суммарным рейтингом, которая принадлежит источнику с максимальным рейтингом в этой группе. 2) Сценарий завершает работу. Если нет, то: 1) Формируются выходные параметры сценария в виде записи, принадлежащей одной из групп с максимальным суммарным рейтингом, которая принадлежит источнику с максимальным рейтингом для этих групп. 2) Сценарий завершает работу

4.2.4.2 Сценарий определения, является ли IP-адрес Tor/Proxy-узлом

Сценарий использует данные таблиц Toripv4, Toripv6, Proxyipv4, Proxyipv6 (см. раздел 4.3.4). Сценарий одинаково работает как для Tor-узлов, так и для Proxy-узлов – независимо от версии IP-адресов.

Входными параметрами сценария являются:

- IP-адрес;
- дата и время, на которое запрашивается признак принадлежности Tor/Proxy-узлу.

Выходным параметром сценария является признак принадлежности IP-адреса Tor/Proxy-узлу:

- TRUE – является Tor/Proxy-узлом;
- FALSE – нет информации о том, что IP-адрес является Tor/Proxy-узлом.

Сценарий возвращает TRUE при условии, что в таблице присутствует хотя бы одна запись запрашиваемого IP-адреса, дата обновления которой больше или равно Ч1 и меньше или равна Ч2, где:

- Ч1 – дата запроса с указанием времени 00:00:00.000;
- Ч2 – дата запроса с указанием времени 23:59:59.999.

Иначе алгоритм возвращает FALSE.

Например, дата запроса 12.05.2020. В этом случае Ч1=12.05.2020 00:00:00.00, Ч2=12.05.2020 23:59:59.999

4.2.4.3 Сценарий поиска контролируемого ресурса по доменному имени

Сценарий в качестве выходных параметров возвращает записи из таблицы superviseddomain (см. раздел 4.3.4).

В таблице 5 приведено описание сценария.

Таблица 5 – Сценарий определения совпадения доменных имен

№	Шаг сценария
1.	Выполняется проверка условия, что искомое доменное имя является доменом первого уровня. Если да, то: 1) Возвращается пустой набор данных. 2) Сценарий завершает работу. Если нет, то переход к следующему шагу
2.	Выполняется поиск искомого доменного имени по условию равенства с доменными именами в таблице superviseddomain. Сравнение выполняется без учета регистра букв. Искомое доменное имя найдено? Если да, то: 1) Возвращаются найденные записи. 2) Сценарий завершает работу. Если нет, то переход к следующему шагу
3.	У искомого доменного имени слева отрезается часть текста, включая первую слева точку, после этого – переход к шагу 1

4.3 Сведения об подсистемах и их частях, необходимых для обеспечения их функционирования

4.3.1 Журналы событий

В Подсистеме предусмотрено два журнала:

- журнал событий API, связанный с событиями использования программного интерфейса Подсистемы;
- журнал событий, связанный с событиями загрузки данных интернет-источников в базу данных модуля «Справочник GeoIP» и удаления устаревших данных.

Программные средства разработки, которые использовались при создании GeoIP, включают в себя средства регистрации следующих событий API:

- вызов API;
- появление ошибок в результате работы API.

Журнал событий загрузки и удаления устаревших данных содержит следующую информацию:

- дата и время события;
- категория события;
- вид события;
- информация события

Журнал событий загрузки и удаления устаревших данных интернет-источников хранится в базе данных модуля «Справочник GeoIP» в таблице event_log (см. структуру таблицы в разделе 4.3.4).

В этом журнале фиксируются события следующих категорий:

- 1) Загрузка файлов. События работы загрузчиков, которые загружают файлы в базу данных модуля «Справочник GeoIP» (см. раздел 0).
- 2) Удаление файлов. События удаления устаревших файлов (см. раздел 4.2.3.3).

В таблице 6 приведено описание категорий событий загрузки.

Таблица 6 – Категории событий GeoIP

Категория события	Вид события	Информация события
Загрузка файлов	Начало загрузки	<имя_загружаемого_файла>
	Завершение загрузки	<имя_загружаемого_файла>
	Ошибка	<имя_загружаемого_файла> <причина_ошибки>
Удаление файлов	Файл удален	<имя_удаленного_файла>
	Ошибка	<имя_удаляемого_файла> <причина_ошибки>

4.3.2 Конфигурационные файлы

Для настройки применяются следующие конфигурационные файлы:

- settings.py – представляет собой конфигурационный файл GeoIP;
- jet-geoip.conf – предназначен для настройки работы программ-скачивателей.

В конфигурационном файле GeoIP:

- 1) Указаны имена источников для GeoIP, ASN и Tor/Proxy-данных.
- 2) Для каждого источника указана гиперссылка на интернет-сайт источника для отображения в модуле «ГПИ» (см. раздел 4.2.2).
- 3) Каждому источнику GeoIP-данных присвоен рейтинг, который используется для определения наиболее вероятного географического местоположения IP-адреса (см. раздел 4.2.4.1).
- 4) Настраивается диапазон времени, используемый в предоставлении наиболее вероятного местоположения IP-адреса.
- 5) Для файлов, созданных программами-скачивателями (см. раздел 4.2.1), указывается информация о том:
 - из какого месторасположения файлы перемещаются с помощью процедуры переноса файлов (см. раздел 4.2.3.2);
 - в какое месторасположение файлы перемещаются с помощью процедуры переноса файлов (см. раздел 4.2.3.2).
- 6) Для файлов, успешно загруженных в базу данных модуля «Справочник GeoIP», указывается месторасположение, куда успешно загруженные файлы перемещаются загрузчиками (см. раздел 0).
- 7) Для файлов, которые не удалось загрузить в модуль «Справочник GeoIP», указывается месторасположение, куда они перемещаются загрузчиками (см. раздел 0).
- 8) Для загрузчиков предусмотрен параметр, который определяет размер порции, которыми загружаются файлы данных в базу данных модуля «Справочник GeoIP». Размер порций измеряется количеством записей.
- 9) Указываются значения параметров сценария определения, является ли IP-адрес Tor/Proxy-узлом (см. раздел 4.2.4.2):
 - количество часов до даты и времени запроса признака Tor/Proxy;
 - количество часов после даты и времени запроса признака Tor/Proxy;Если параметры не указаны, то им присваиваются значения по умолчанию (значения по умолчанию приведены в описании сценария определения, является ли IP-адрес Tor/Proxy-узлом, в разделе 4.2.4.2).
- 10) Указывается срок хранения данных, по истечению которого устаревшие данные подлежат удалению (см. раздел 4.2.3.3).

Конфигурационный файл jet-geoip.conf предназначен для настройки работы программ-скачивателей.

В файле используются секции:

1) [downloaders] – общая для всего приложения.

Ключи секции:

- logging_conf – путь к настройкам записи логов;
- source_order – порядок загрузки по умолчанию;
- maxmind_license_key – ключ для получения данных источника MAXMIND.

2) [MaxmindCity], [MaxmindAsn], [DBip], [TorProject], [TheSpeedX] – имеют одинаковую структуру.

Ключи секции:

- download_url – ссылка на источник;
- download_path – место сохранения полученных данных;
- processed_path_ – путь к местоположению CSV-файлов, подготовленных к загрузке в базу данных модуля «Справочник GeoIP»;
- src – имя источника.

4.3.3 Интернет-источники

GeoIP-данные в базе данных модуля «Справочник GeoIP» обновляются в соответствии с графиком обновления данных в интернет-источниках. Описание интернет-источников GeoIP-данных приведены в таблице 7.

Таблица 7 – Источники GeoIP-данных

Источник	База	Ссылка	Платная	Обновляется
MAXMIND	GeoLite2 City	https://dev.maxmind.com/geoip/geoip2/geolite2/	Нет	1 раз в неделю
DBIP	IP to City Lite	https://db-ip.com/db/download/ip-to-city-lite	Нет	Ежедневно

Tor/Proху-данных в базе данных модуля «Справочник GeoIP» обновляются один раз в день. Описание интернет-источников приведено в таблицах 8 и 9. Интернет-источники бесплатные.

Таблица 8 – Интернет-источники списков Tor-узлов

Источник	Ссылка
TorNodes	https://www.dan.me.uk/Torlist/
TORPROJECT	https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1

Таблица 9 – Интернет-источники Proху-узлов

Источник	Ссылка
PROXYLIST	https://www.Proxy-list.download/
GHProxyList	https://raw.githubusercontent.com/clarketm/Proxy-list/master/Proxy-list-raw.txt
TheSpeedX	https://raw.githubusercontent.com/TheSpeedX/SOCKS-List/master

4.3.4 База данных

Для хранения данных в модуле «Справочник GeoIP» используется реляционная СУБД PostgreSQL.

Данные в источниках GeoIP поступают в виде блоков IP-адресов:

- в формате CIDR;
- в виде диапазона IP-адресов, представленного первым и последним IP-адресами.

Для каждого отдельного блока IP-адреса в базе данных хранятся записи для каждой даты обновления. Таким образом обеспечивается хранение истории изменений GeoIP-данных. Исторические данные территориального распределения IP-адресов сети Интернет хранятся в течение одного года. По истечению срока хранения устаревшие данные удаляются (об удалении устаревших данных см. в разделе 4.2.3.3).

В таблицах 10–16 приведена структура таблиц базы данных модуля «Справочник GeoIP».

Таблица 10 – Структура таблицы geoipv4 – GeoIP-данные IPv4

Атрибут	Поле	Тип	Обязательность
Источник	src	Строка	Да
Дата и время обновления	updated_at	Дата и время	Да
Первый IP-адрес блока	ip_first	IPv4	Да
Последний IP-адрес блока	ip_last	IPv4	Да
Подсеть	subnet	Строка	Да
Код страны	country_code	Строка	Да
Страна	country_name	Строка	Да
Регион	region_name	Строка	Нет
Город/населенный пункт	city_name	Строка	Нет
Интернет-провайдер	internet_service_provider_name	Строка	Нет
Организация	organization_name	Строка	Нет
Признак корневого DNS-сервера	is_anycast	Перечисляемый («Y» – является; «N» – не является «U» – не определено)	Нет

Таблица geoipv6 имеет структуру, аналогичную таблице geoipv4 (Таблица 10).

Таблица 11 – Структура таблицы toripv4 – список IP-адресов Tor IPv4

Атрибут	Поле	Тип	Обязательность
Источник	src	Строка	Да
Дата обновления	updated_at	Дата и время	Да
IP-адрес	ip	IPv4	Да

Таблицы toripv6, proxiipv4, proxiipv6 имеют структуру, аналогичную таблице toripv4 (Таблица 11).

Таблица 12 – Структура таблицы supervisedipv4 – IP-адреса контролируемых ресурсы IPv4

Атрибут	Поле	Тип	Обязательность
Дата и время изменения статуса контроля	updated_at	Дата и время	Да
Первый IP-адрес блока	ip_first	IPv4	Да
Последний IP-адрес блока	ip_last	IPv4	Да
Подсеть	subnet	Строка	Да
Идентификатор организации	org_id	Строка	Да
Статус контроля	is_supervised	Логический тип	Да

Таблица supervisedipv6 имеет структуру, аналогичную таблице supervisedipv4 (Таблица 12).

Таблица 13 – Структура таблицы superviseddomain – доменные имена контролируемых ресурсов

Атрибут	Поле	Тип	Обязательность
Дата и время изменения статуса контроля	updated_at	Дата и время	Да
Доменное имя	fqdn	Строка	Да
Идентификатор организации	org_id	Число	Да
Статус контроля	is_supervised	Логический тип	Да

Таблица 14 – Структура таблицы asnipv4 – автономные системы IPv4

Атрибут	Поле	Тип	Обязательность
Источник	src	Строка	Да
Дата и время обновления	updated_at	Дата и время	Да
Первый IP-адрес сети	ip_first	IPv4	Да
Последний IP-адрес сети	ip_last	IPv4	Да
Подсеть	subnet	Строка	
Номер автономной системы	asn	Строка	Да
Данные о владельце IP-адресов автономной системы	asn_info	Строка	Да

Таблица asniprv6 имеет структуру, аналогичную таблице asniprv4 (Таблица 14).

Таблица 15 – Структура таблицы event_log – журнал событий подсистемы

Атрибут	Поле	Тип	Обязательность
Дата и время события	created_at	Дата и время	Да
Категория события	event_categ	Строка	Да
Вид события	event_type	Строка	Да
Информация события	event_info	Строка	
Источник	src	Строка	Да
Вид данных	type	Строка	Да
Количество записей	records	Целое	Да, для категории события «Загрузка файла»

В таблице 16 приведена структура таблицы comments, предназначенная для хранения комментариев к IP-адресам (см. раздел 4.2.2.7).

Таблица 16 – Структура таблицы comments – комментарии

Атрибут	Поле	Тип	Обязательность
IP-адрес	ip	Строка	Да
Комментарий	comment	Текстовый	Да
Время внесения комментария	created	Метка времени	Да
IP-адрес комментатора	creator_ip	Строка	Да

4.3.5 Программные интерфейсы

Подсистема предоставляет данные посредством программного интерфейса (API), включая следующую информацию:

- наиболее вероятное местоположении IP-адреса на выбранную дату, включая владельцев IP-адреса, признаки принадлежности IP-адреса Tor/Proху-узлам и контролируемым ресурсам с помощью API /geoip/pref_location;
- развернутые данные географического местоположения IP-адреса на выбранную дату с помощью API /geoip/detail/{ip_addr};
- историю изменения географического местоположения IP-адреса с помощью API /geoip/history/{source}/{ip_addr};
- признак принадлежности IP-адреса контролируемым ресурсам на выбранную дату с помощью /supervised/ips;
- признак принадлежности доменного имени контролируемым ресурсам на выбранную дату с помощью /supervised/domains;
- историю загрузки файлов обновлений с помощью API /geoip/logs_history.

Кроме того, перечисленные выше API использует модуль «ГПИ» для получения данных. Ниже приведено описание API, которое выполнено в соответствии со спецификацией swagger 2.0.

```
swagger: "2.0"
info:
  description: "GeoIP"
  version: "0.0.0"
  title: "GeoIP"
  contact:
    email: "user@jet.su"
host: "localhost"
basePath: "/api/"

schemes:
- "http"
paths:
  /geoip/pref_location:
    post:
      tags:
        - geoip
      summary: "Наиболее вероятное местоположение"
      description: >
        "Отображение списка пар IP:дата в список пар IP:данные локации"
      consumes:
        - "application/json"
      produces:
        - "application/json"
      parameters:
        - in: "body"
          name: "body"
          required: true
          schema:
            type: "object"
            properties:
              date:
                type: "string"
                format: "date-time"
              ips:
                type: "array"
                items:
                  type: "string"
      responses:
        200:
          description: "Success"
          schema:
            type: "array"
            items:
              $ref: '#/definitions/PrefLocation'
```

```

/geoip/detail/{ip_addr}:
  get:
    tags:
      - geoip
    summary: "Развернутые данные местоположения"
    description: "Развернутые данные местоположения"
    consumes:
      - "application/json"
    produces:
      - "application/json"
    parameters:
      - in: "path"
        name: "ip_addr"
        required: true
        type: "string"
        description: "IP-адрес"
      - in: "query"
        required: false
        name: "date"
        type: "string"
        format: "date-time"
        description: >
          "дата и время, на которое запрашиваются GeoIP-данные для IP-
адреса."
    responses:
      200:
        description: "Success"
        schema:
          $ref: '#/definitions/IPLocationDetail'

/geoip/history/{source}/{ip_addr}:
  get:
    tags:
      - geoip
    summary: "Исторические данные местоположения"
    description: "Исторические данные местоположения"
    consumes:
      - "application/json"
    produces:
      - "application/json"
    parameters:
      - in: "path"
        name: "ip_addr"
        required: true
        type: "string"
        description: "IP-адрес"
      - in: "path"
        name: "source"

```

```

        required: true
        type: "string"
        description: "источник GeoIP-данных"
    - in: "query"
      name: "up_to_date"
      type: "string"
      description: "Дата до которой выбирать данные"
      required: false
    - in: "query"
      name: "offset"
      type: "string"
      description: "Номер страницы"
      required: false
    - in: "query"
      name: "size"
      type: "string"
      description: "Количество записей на страницу"
      required: false
  responses:
    200:
      description: "Success"
      schema:
        type: "object"
        properties:
          totalCount:
            type: "integer"
          data:
            type: "array"
            items:
              $ref: '#/definitions/IPLocationHistory'
    404:
      description: "Not found"

/geoip/asn_history/{source}/{ip_addr}:
  get:
    tags:
      - geoip
    summary: "Исторические данные ASN"
    description: "Исторические данные ASN"
    consumes:
      - "application/json"
    produces:
      - "application/json"
    parameters:
      - in: "path"
        name: "ip_addr"
        required: true
        type: "string"
        description: "IP-адрес"

```

- in: "path"
 - name: "source"
 - required: true
 - type: "string"
 - description: "источник ASN-данных"
- in: "query"
 - name: "up_to_date"
 - type: "string"
 - description: "Дата до которой выбирать данные"
 - required: false
- in: "query"
 - name: "offset"
 - type: "string"
 - description: "Номер страницы"
 - required: false
- in: "query"
 - name: "size"
 - type: "string"
 - description: "Количество записей на страницу"
 - required: false

responses:

- 200:
- description: "Success"
 - schema:
 - type: "object"
 - properties:
 - totalCount:
 - type: "integer"
 - data:
 - type: "array"
 - items:
 - \$ref: '#/definitions/ASN'
- 404:
- description: "Not found"

/geoip/logs_history:

- get:
- tags:
 - geoip
 - summary: "История загрузки файлов обновлений"
 - description: "История загрузки файлов обновлений"
 - consumes:
 - "application/json"
 - produces:
 - "application/json"

```

parameters:
  - in: "query"
    required: false
    name: "date"
    type: "string"
    format: "date-time"
    description: "дата и время"
  - in: "query"
    required: false
    name: "source"
    type: "string"
    description: "источник"
  - in: "query"
    required: false
    name: "source_type"
    type: "string"
    description: "Тип данных"
responses:
  200:
    description: "Success"
    schema:
      type: "object"
      properties:
        totalCount:
          type: "integer"
        data:
          type: "array"
          items:
            type: "object"
            properties:
              updated_at:
                type: "string"
                format: "date-time"
              source:
                type: "string"
              source_type:
                type: "string"
              proccessed_record:
                type: "integer"
              event_info:
                type: "string"
              event_type:
                type: "string"
              source_url:
                type: "string"

```

```

/supervised/ips:
  post:
    parameters:
      - in: "body"
        name: "body"
        required: true
        schema:
          type: "object"
          properties:
            date:
              type: "string"
              format: "date-time"
            ips:
              type: "array"
              items:
                type: "string"
    responses:
      200:
        description: "Success"
        schema:
          type: "object"
          properties:
            ip_value:
              type: "array"
              items:
                type: "string"

    tags:
      - supervised
    consumes:
      - "application/json"
    produces:
      - "application/json"

/supervised/domains:
  post:
    parameters:
      - in: "body"
        name: "body"
        required: true
        schema:
          type: "object"
          properties:
            date:
              type: "string"
              format: "date-time"
            fqdns:
              type: "array"

```

```

        items:
            type: "string"
responses:
  200:
    description: "Success"
    schema:
      type: "array"
      items:
        type: "object"
        properties:
          fqdn:
            type: "string"
          orgs:
            type: "array"
            items:
              type: object
              properties:
                org_id:
                  type: "string"
tags:
  - supervised
consumes:
  - "application/json"
produces:
  - "application/json"

definitions:
  ASN:
    type: "object"
    properties:
      asn:
        type: "string"
      owner:
        type: "string"
      subnet:
        type: "string"
      updated_at:
        type: "string"
        format: "date-time"

  IPVersion:
    type: "string"
    description: "версия IP-адреса"
    enum:
      - "IPv4"
      - "IPv6"

```

```

FQDNDate:
  type: "object"
  properties:
    fqdn:
      type: "string"
    date:
      type: "string"
    description: >
      "дата и время, на которое запрашиваются признак"

IPDate:
  type: "object"
  properties:
    ip:
      type: "string"
    date:
      type: "string"
    description: >
      "дата и время, на которое запрашиваются признак"

IPRange:
  type: "object"
  description: >
    "блок IP-адресов в виде диапазона, определенного начальным и
конечным IP-адресами;"
  properties:
    ip_first:
      type: "string"
    ip_last:
      type: "string"

IPLocationHistory:
  type: "object"
  properties:
    updated_at:
      type: "string"
      format: "date-time"
      description: "дата и время обновления"
    subnet:
      description: >
        "блок IP-адресов, в который входит IP-адрес в формате CIDR;"
      type: "string"
    ip_range:
      $ref: '#/definitions/IPRange'
    country:
      description: "наименование страны нахождения IP-адреса"
      type: "string"

```

```

region:
  description: "наименование региона нахождения IP-адреса"
  type: "string"
city:
  description: "наименование города нахождения IP-адреса"
  type: "string"
isp:
  description: "наименование провайдера"
  type: "string"
asns:
  description: >
    "массив автономных систем, содержащий в каждом элементе
    номер автономной системы и наименование автономной системы"
  type: "array"
  items:
    $ref: '#/definitions/ASN'
is_tor_node:
  type: "boolean"
  description: >
    "признак принадлежности Tor"
is_proxy:
  type: "boolean"
  description: >
    "признак принадлежности Proxy"
is_supervised:
  type: "boolean"
  description: >
    "признак принадлежности контролируемому ресурсу"

IPLocationDetail:
  type: "object"
  properties:
    address_version:
      $ref: '#/definitions/IPVersion'
    ipaddress:
      description: "IP-адрес"
      type: "string"
    is_tor_node:
      type: "boolean"
      description: >
        "признак принадлежности Tor"
    is_proxy:
      type: "boolean"
      description: >
        "признак принадлежности Proxy"
    is_supervised:
      type: "boolean"
      description: >
        "признак принадлежности контролируемому ресурсу"

```

```

    ip_locations:
      type: "array"
      items:
        $ref: '#/definitions/IPLocation'

IPLocation:
  type: "object"
  properties:
    source:
      type: "string"
      description: "Имя источника"
    rating:
      type: "number"
      format: "float"
      description: "рейтинг источника"
    updated_at:
      type: "string"
      format: "date-time"
      description: "дата и время обновления"
    subnet:
      description: >
        "блок IP-адресов, в который входит IP-адрес в формате CIDR;"
      type: "string"
    ip_range:
      $ref: '#/definitions/IPRange'
    country:
      description: "наименование страны нахождения IP-адреса"
      type: "string"
    region:
      description: "наименование региона нахождения IP-адреса"
      type: "string"
    city:
      description: "наименование города нахождения IP-адреса"
      type: "string"
    isp:
      description: "наименование провайдера"
      type: "string"
    asns:
      description: >
        "массив автономных систем, содержащий в каждом элементе
        номер автономной системы и наименование автономной системы"
      type: "array"
      items:
        $ref: '#/definitions/ASN'

PrefLocation:
  type: "object"

```

```

properties:
  source:
    type: "string"
    description: "Имя источника"
  rating:
    type: "number"
    format: "float"
    description: "рейтинг источника"
  updated_at:
    type: "string"
    format: "date-time"
    description: "дата и время обновления"
  ipaddress:
    description: "IP-адрес"
    type: "string"
  subnet:
    description: >
      "блок IP-адресов, в который входит IP-адрес в формате CIDR;"
    type: "string"
  ip_range:
    $ref: '#/definitions/IPRange'
  country:
    description: "наименование страны нахождения IP-адреса"
    type: "string"
  region:
    description: "наименование региона нахождения IP-адреса"
    type: "string"
  city:
    description: "наименование города нахождения IP-адреса"
    type: "string"
  isp:
    description: "наименование провайдера"
    type: "string"
  address_version:
    $ref: '#/definitions/IPVersion'
  asns:
    description: >
      "массив автономных систем, содержащий в каждом элементе
      номер автономной системы и наименование автономной системы"
    type: "array"
    items:
      $ref: '#/definitions/ASN'
  is_tor_node:
    type: "boolean"
    description: >
      "признак принадлежности Tor"
  is_proxy:
    type: "boolean"
    description: >

```

```

        "признак принадлежности Proxy"
    is_supervised:
        type: "boolean"
        description: >
            "признак принадлежности контролируемому ресурсу"
    supervised_orgs:
        type: "array"
        items:
            type: "object"
            properties:
                org_id:
                    type: string

description: >
    "признак принадлежности контролируемому ресурсу"

```

API при выполнении запросов возвращает стандартные для HTTP коды ответов.

4.3.6 Состав технических и программных средств

Компоненты GeoIP располагаются на трех виртуальных серверах.

Информационный обмен между компонентами GeoIP выполняется средствами сети передачи данных с использованием стека протоколов TCP/IP. Скорость обмена информацией между компонентами должна быть обеспечена на уровне – не менее 100 Мб/с на протяжении всего срока эксплуатации GeoIP.

Параметры информационного обмена между компонентами GeoIP приведены в таблице 17.

Таблица 17 – Параметры информационного обмена между компонентами GeoIP

Протокол:Порт	Описание
TCP:80	Взаимодействие пользователя с модулем «Графический пользовательский интерфейс»
TCP:443	Перенос GeoIP-файлов, ASN-файлов, Tor/Proxy-файлов
TCP:22	Взаимодействие с базой данных

Характеристики виртуального сервера 1 приведены в таблице 18.

Таблица 18 – Требования к техническому обеспечению сервера 1

Параметр	Описание
Операционная система	Ubuntu LTS
Процессор	4 ядра
Память	16 ГБ
Диск	500 ГБ

Характеристики виртуального сервера 2 приведены в таблице 19.

Таблица 19 – Требования к техническому обеспечению сервера 2

Параметр	Описание
Операционная система	Ubuntu LTS
Процессор	8 ядер
Память	32 ГБ
Диск	500 ГБ

Характеристики виртуального сервера 3 приведены в таблице 20.

Таблица 20 – Требования к техническому обеспечению сервера 3

Параметр	Описание
Операционная система	Ubuntu LTS
Процессор	20 ядер
Память	32 ГБ
Диск	2 ТБ

Программное обеспечение необходимое для функционирования GeolP:

- 1) ОПО «Jet GEO IP»;
- 2) Операционная система Ubuntu LTS;
- 3) СУБД PostgreSQL;
- 4) Программа cron для реализации функций модуля «Планировщик»;
- 5) Программа gzip для архивирования файлов данных после их успешной загрузки в базу данных модуля «Справочник GeolP»;
- 6) Браузер для выполнения функций, представленных в модуле «ГПИ». Подсистема совместима с браузерами Chrome.

Для функционирования GeolP требуются следующие программные библиотеки:

- docker;
- docker-compose.

5 Перечень принятых сокращений

Сокращение	Описание
API	От англ. Application Programming Interface – программный интерфейс, представляющий собой набор программных функций для взаимодействия систем
ASN	От англ. Autonomous System Number – автономная система, т. е. система IP-сетей и маршрутизаторов, которыми управляют один или несколько операторов и которые имеют единую политику маршрутизации
CIDR	От англ. Classless Inter-Domain Routing – метод бесклассовой междоменной маршрутизации
CSV	От англ. Comma-Separated Values – текстовый формат, который предназначен для представления табличных данных. Строка таблицы соответствует строке текста, которая содержит одно или несколько полей, разделенных символами разделителями, например, запятыми
DNS	От англ. Domain Name System – система доменных имен
FQDN	От англ. Fully Qualified Domain Name – полностью определенное имя домена, т. е. то, которое включает в себя имена всех родительских доменов иерархии DNS
HTTP	От англ. HyperText Transfer Protocol – группа протоколов прикладного уровня на основе гипертекста для передачи произвольных данных. Включает различные версии протокола Http, Http/2, Https
JSON	От англ. JavaScript Object Notation – текстовый формат структурированного обмена данными, легко читаемый людьми
PDF	От англ. Portable Document Format – межплатформенный открытый формат электронных документов, изначально разработанный фирмой Adobe Systems с использованием ряда возможностей языка PostScript
SFTP	От англ. SSH File Transfer Protocol – защищенный протокол передачи файлов
TCP	От англ. Transmission Control Protocol – сетевой протокол передачи данных
БД	База данных
ГПИ	Графический пользовательский интерфейс
ИБП	Источник бесперебойного питания
ИНН	Идентификационный номер налогоплательщика – уникальный номер, упорядочивающий учет налогоплательщиков в Российской Федерации
НСД	Несанкционированный доступ
ОПО	Общее программное обеспечение
СУБД	Система управления базами данных
ТИ	Техническая инфраструктура
ТО	Техническое обслуживание

6 Перечень терминов

Термин	Описание
ASN-данные	Информация об автономных системах: номер автономной системы; владелец IP-адресов автономной системы
ASN-файл	Файл, полученный в результате скачивания специальными программами ASN-данных из открытых интернет-источников
GeoIP-данные	Информация о географическом местоположении IP-адресов сети Интернет, содержащих информацию: о стране и городе расположения IP-адреса; владельцах IP-адресов
GeoIP-файл	Файл, полученный в результате скачивания специальными программами GeoIP-данных из открытых интернет-источников
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP. В версии протокола IPv4 IP-адрес имеет длину 4 байта, а в версии протокола IPv6-16 байт
SFTP-протокол	Протокол прикладного уровня, который предназначен для копирования и выполнения других операций с файлами, который использует безопасное соединение
Tor/Proxy-данные	Список IP-адресов, которые принадлежат: прокси-серверам или прокси-серверам, которые позволяют устанавливать анонимное сетевое соединение с помощью специального программного обеспечения Tor (сокр. от англ. The Onion Router)
Tor/Proxy-файл	Файл, полученный в результате скачивания специальными программами Tor/Proxy-данных из открытых интернет-источников
Владелец IP-адреса	Организация-оператор автономной системы, которая владеет IP-адресом сети Интернет
Доменное имя	Символьное имя, служащее для идентификации областей, которые являются единицами административной автономии в сети Интернет, в составе вышестоящей по иерархии такой области. Каждая такая область называется доменом. Общее пространство имен сети Интернет функционирует на базе DNS – системы доменных имен. Доменные имена дают возможность адресации интернет-узлов и расположенным на них сетевым ресурсам (веб-сайтам, серверам электронной почты, другим службам) быть представленными в удобной для человека форме
Контролируемый ресурс	Информационный ресурс сети Интернет, который принадлежит контролируемым субъектам и находится под особым контролем. Подсистема использует информацию об IP-адресах и доменных именах контролируемых ресурсов