УДК 004.056.53

С. В. Поршнев, О. А. Пономарева, Э. В. Соломаха

КАРТОГРАФИЧЕСКИЙ МОДУЛЬ ДЛЯ ВИЗУАЛИЗАЦИИ МЕСТОПОЛОЖЕНИЯ IP-АДРЕСОВ

В связи с непрерывно увеличивающимся числом сетевых атак и, соответственно, объемов работ, выполняемых специалистами-аналитиками, по выявлению лиц, нарушающих безопасность объектов критической информационной инфраструктуры, разработка программных инструментов, обеспечивающих визуализацию анализируемой при этом информации, является актуальной. В статье описан картографический модуль, обеспечивающий по заданному IP-адресу поиск в общедоступных БД компаний MaxMind, БД 3WiFi, WHOIS информации о данном IP-адресе, визуализацию его местоположения на электронной географической карте и текстовую информацию о стране и городе его нахождения, а также провайдере, предоставившем данный IP-адрес. Данный модуль реализован в виде web-сервера с помощью веб-фреймворка Django. Приведен пример, иллюстрирующий выбранные способы визуализации информации, относящейся к выбранному IP-адресу. Определены направления его дальнейшего развития.

Due to the continuously increasing number of network attacks and, accordingly, the volume of work performed by analysts to identify individuals who violate the security of critical information infrastructure objects, the development of software tools that provide visualization of the information analyzed in this case is relevant. A cartographic module is described that provides a search for publicly accessible databases of MaxMind companies, 3WiFi databases, WHOIS information for this IP-address, visualization of its location on an electronic geographic map and text information about the country and city of its location using the specified IP-address , as well as the provider that provided this IP-address. This module is implemented as a WEB server using the Django web framework. An example is provided illustrating selected methods for visualizing information related to a selected IP-address. The directions of its further development are determined.

Ключевые слова: IP-адрес, сетевая атака, база данных, географическая карта.

Keywords: IP-address, network attack, database, geographical map.

Введение

Анализ общедоступных статистических данных, размещаемых в том числе на сайте лаборатории Касперского [1], свидетельствует о непрерывном увеличении числа предпринимаемых сетевых атак, несмотря на существующие многочисленные технические решения для защиты

пользовательских информационных ресурсов от вредоносных воздействий. Например, сравнение числа зарегистрированных лабораторией Касперского атак в течение 2018 и 2019 гг. обнаруживает более чем двукратное увеличение числа среднемесячных атак: с 1 млн атак до 2 и более млн в сутки, часть из которых оказались успешными.

Для анализа возникающих угроз ИБ той или иной компьютерной сети и прогнозирования вероятных направлений следующих действий злоумышленника специалисту-аналитику, занимающемуся вопросами противодействия сетевым атакам, необходимо иметь информацию о координатах местоположения IP-адреса, с которого предпринята попытка атаки (соответственно, стране и городе, в котором он находится), а также информацию о провайдере, владеющем данным IP-адресом.

В этой связи разработка программного инструмента, обеспечивающего визуализацию на электронных картах местоположения IP-адреса и вывод соответствующей текстовой информации, оказывается актуальной. В статье обсуждается разработанный картографический модуль для визуализации местоположения IP-адресов и отображения актуальной тестовой информации о данном IP-адресе.

Источники информации об IP-адресах

Для разработки картографического модуля были использованы следующие источники.

1. Базы данных (БД) компании *MaxMind* [4], для доступа к которым использовалось приложение MaxMind DB Python Module [5]:

а) GeoIP2-City, содержащая информацию о принадлежности IP-адресов городам с указанием почтового индекса, страны и континента;

б) GeoIP2-Connection-Type, содержащая информацию, позволяющую по IP-адресу идентифицировать тип подключения посетителей вашего сайта;

в) GeoIP2-Country, содержащая информацию, позволяющую идентифицировать страну, которой принадлежит IP-адрес;

г) GeoIP2-ISP, содержащая информацию, позволяющую идентифицировать провайдера услуг Интернета, название организации, протокол, используемый для подключения к сети интернет, IP-адрес провайдера.

2. БД 3WiFi [6], содержащая информацию о беспроводных точках доступа в Интернет. Данный ресурс поддерживается и наполняется сообществом пользователей (технология краудсорсинга), осуществляющих сканирование беспроводных точек доступа в Интернет.

3. БД WHOIS [7] интернет-регистратора RIPE NCC, отвечающего за Европейский регион и часть Азиатского [3].

Содержание контента основных полей обсуждаемых БД представлено в таблице.

Содержание контента основных полей, используемых БД

База данных	Содержание контента
GeoIP2-City	континент
	страна регистрации
	область
	город
	почтовый индекс
	географические широта и долгота
GeoIP2-Connection-Type	континент
	страна
	страна регистрации
	тип подключения
GeoIP2-Country	континент
	страна
	страна регистрации
GeoIP2-ISP	провайдер
	организация
3WiFi	дата добавления информации о точке беспроводного доступа в Интернет в БД
	принадлежность к диапазону IP-адресов / 16
	MAC-адрес сети точки доступа
	имена сети точки доступа
	тип защиты точки доступа
	ключ сети
	географические широта и долгота
WHOIS	континент
	страна
	город
	локация
	провайдер

Структурная схема картографического модуля

Структурная схема картографического модуля представлена на рисунке 1. В первую очередь для разрабатываемого картографического модуля была создана структурная схема, отображающая взаимосвязь отдельных компонентов модуля.

Из рисунка 1 видно, что взаимодействие пользователя с картографическим модулем обеспечивает web-сервер, разработанный с использованием веб-фреймворка *Django* [9], который является инструментом быстрой разработки сайтов.

Сервер обеспечивает создание запроса и осуществляет поиск информации, релевантной данному запросу, в одной из описанных в предыдущем разделе БД.

Для отображения местоположения IP-адреса на географической карте с помощью библиотеки Leaflet [2] web-сервер обращается к ло-

кальному хранилищу карт, в котором хранятся электронные географические карты, загруженные с ресурса *OpenStreetMap* [3]. Технология создания подобных хранилищ описана в [10].

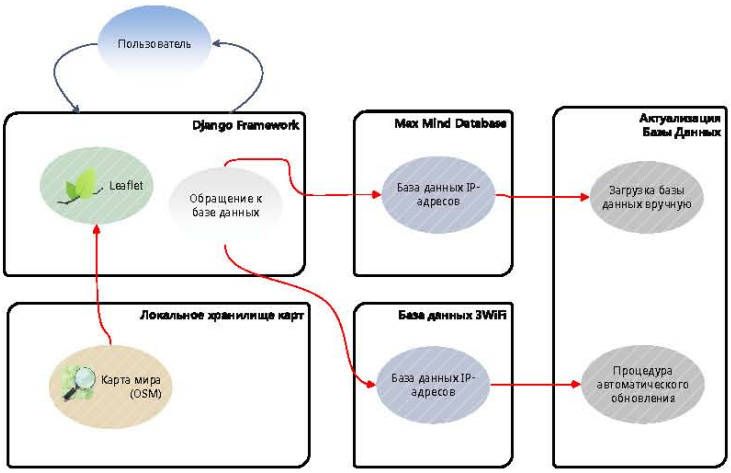

Рис. 1. Структурная схема картографического модуля

Отметим, что при использовании локальных БД, содержащих информацию об адресах, картографический модуль можно использовать без подключения к Интернету. Для этого web-сервер предоставляет режим ручной загрузки БД, а также возможность их автоматического обновления.

Интерфейс пользователя картографического модуля

Скриншот рабочего окна картографического модуля представлен на рисунке 2.

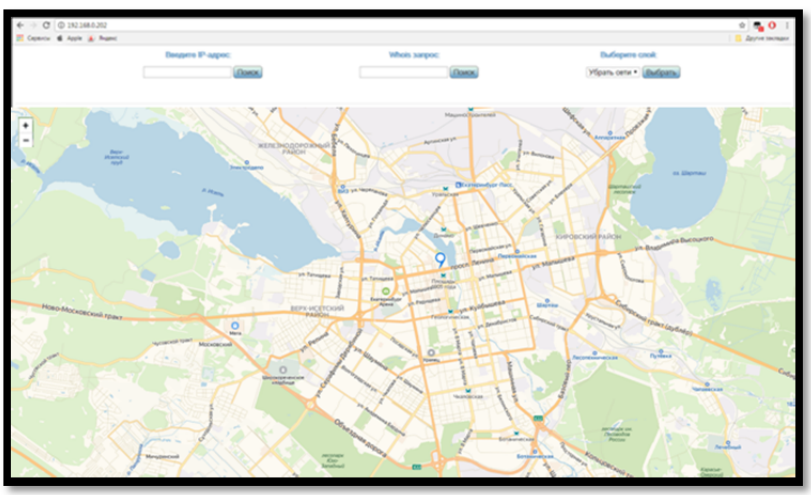

Рис. 2. Интерфейс пользователя

Из рисунка 2 видно, что интерфейс картографического модуля состоит из следующих управляющих элементов: кнопки увеличения масштаба карты; поля ввода IP-адреса и кнопки «Поиск», нажатие на которую инициирует поиск релевантной запросу информации в БД компании *MaxMind*; поля ввода IP-адреса и кнопки «Поиск», нажатие на которую инициирует поиск релевантной запросу информации в БД *WHOIS*; элемента управления слоями, отображаемыми на карте.

Интерфейс web-сервиса после выполнения запроса к БД компании *MaxMind* о поиске координат IP-адреса 95.173.148.66 в режиме вывода тестовой информации, представляющей интерес для специалиста-аналитика, ведущего расследование факта нарушения информационной безопасности, изображен на рисунке 3.

Рис. 3. Отображения информации о выбранном IP-адресе

Направления дальнейшего развития картографического модуля

В настоящее время осуществляется разработка механизма, обеспечивающего интеграцию картографического модуля и модуля анализа сетевого трафика. После этого запланирована разработка следующих дополнительных сервисов картографического модуля:

— отображение на глобальной карте мира информационных потоков, отмеченных системой анализа сетевого трафика как «компьютерные атаки»;

— отображение IP-адресов, которые с высокой долей вероятности могут быть использованы злоумышленником для маскировки своего IP-адреса средствами VPN-туннелей;

— отображение IP-адресов и географического расположения беспроводных точек доступа в Интернет с низкой устойчивостью к перебору паролей (данные точки доступа потенциально могут быть использованы злоумышленником как «входные узлы» для проведения компьютерных атак);

— реализация механизма, позволяющего загружать данные об IP-адресах, полученных от Интернет-провайдеров.

Заключение

Разработанный картографический модуль является инструментом, с помощью которого пользователи могут визуализировать информацию о IP-адресах, находящихся в общедоступных БД, с минимальными временными затратами.

Его дальнейшее развитие обеспечит специалистов-аналитиков удобным инструментом поддержки принимаемых ими решений при расследовании инцидентов, связанных с нарушениями информационной безопасности компьютерных сетей.

Список литературы

1. *Интерактивная* карта киберугроз. URL: https://cybermap.kaspersky.com/ru/stats (дата обращения: 14.10.2019).

2. *Leaflet*: an open-source JavaScript library for mobile-friendly interactive maps. URL: https://leafletjs.com/download.html (дата обращения: 16.10.2019).

3. *Planet* OSM. URL: https://planet.openstreetmap.org/ (дата обращения: 16.10.2019).

4. *GeoLite2* Free Downloadable Databases. URL: https://dev.maxmind.com/ru/geolite2/ (дата обращения: 16.10.2019).

5. *MaxMind* DB Python Module. URL: https://maxminddb.readthedocs.io/en/latest/ (дата обращения: 16.10.2019).

6. *3WiFi* — свободная база точек доступа. URL: https://3wifi.stascorp.com/home (дата обращения: 16.10.2018).

7. *Ripe* NCC. URL: https://www.ripe.net/ (дата обращения: 16.10.2019).

8. *Index* of /ripe/dbase. URL: https://ftp.ripe.net/ripe/dbase/ (дата обращения: 16.10.2019)

9. *Django*. The web framework for perfectionists with deadlines. URL: https://www.djangoproject.com/ (дата обращения: 16.10.2019)

10. *Creating* your own tiles. URL: https://wiki.openstreetmap.org/wiki/Creating_your_own_tiles (дата обращения: 16.10.2019).

Об авторах

Сергей Владимирович Поршнев — д-р техн. наук, проф., Уральский федеральный университет им. первого Президента России Б.Н. Ельцина; ведущ. науч. сотр., Институт математики и механики им. Н.Н. Красовского Уральского отделения Российской академии наук, Россия.

E-mail: s.v.porshnev@urfu.ru

Ольга Алексеевна Пономарева — ст. преп., Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Россия.

E-mail: o.a.ponomareva@urfu.ru

Эдуард Викторович Соломаха — ассист., Уральский федеральный университет им. первого Президента России Б.Н. Ельцина, Россия.

E-mail: o.a.ponomareva@urfu.ru

The authors

Prof. Sergey V. Porshnev, Ural Federal University named after First President of Russia B.N. Yeltsin; Leading Researcher, N.N. Krasovsky Institute of Mathematics and Mechanics of the Ural Branch Russian Academy of Sciences, Russia.
E-mail: s.v.porshnev@urfu.ru

Olga A. Ponomareva, Assistant Professor, Ural Federal University named after First President of Russia B.N. Yeltsin, Russia.
E-mail: o.a.ponomareva@urfu.ru

Eduard V. Solomaha, Assistant, Ural Federal University named after First President of Russia B.N. Yeltsin, Russia.
E-mail: o.a.ponomareva@urfu.ru