РОЗРОБКА ПРОГРАМИ ВИЯВЛЕННЯ НЕДОСТОВІРНИХ ЛОКАЛІЗАЦІЙ IP-АДРЕС У ГЛОБАЛЬНІЙ МЕРЕЖІ

Ілюстративний матеріал

до дипломної роботи

За спеціальністю 7.17010301 – «Управління інформаційною безпекою»

08-42.ДР.007.00.000

Виконала: ст. гр. УБ-15сп Сандулова А.Ю.

Науковий керівник: к.ф.-м.н., доц. Шиян А.А.

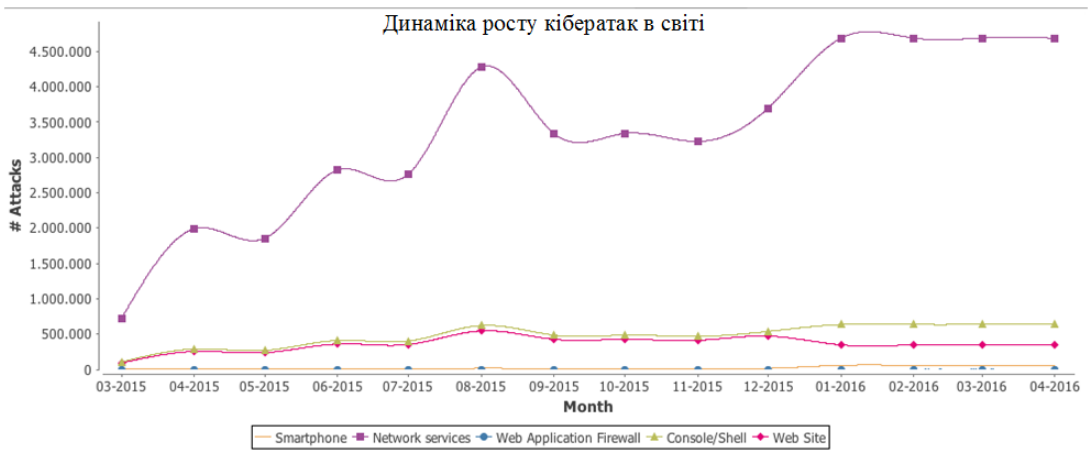
Актуальність

- Загальна інформатизації суспільства призводить до розширення сфери професійного шахрайства, з використання складних сучасних технологій. Як наслідок, виникає потреба в більш швидких і жорстких методах реагування на подібні типи загрози.

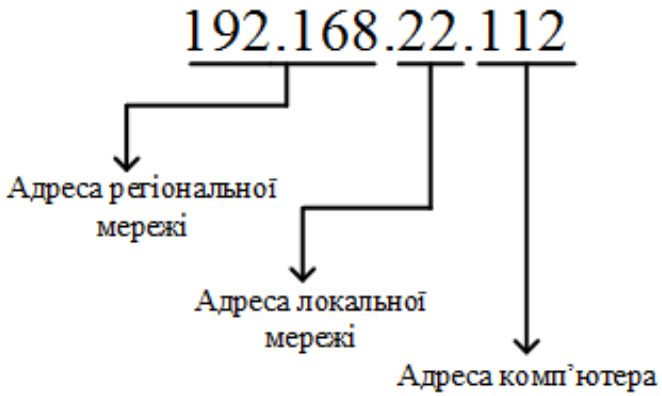
Мета

- Створення унікального інформаційного ресурсу, що дозволяє виявляти недостовірні локалізації IP-адрес у глобальній мережі, і, як наслідок, справжнє місце розташування джерела загрози.

Інтернет-технології мають місце у кожній сфері життя суспільства й особистості.

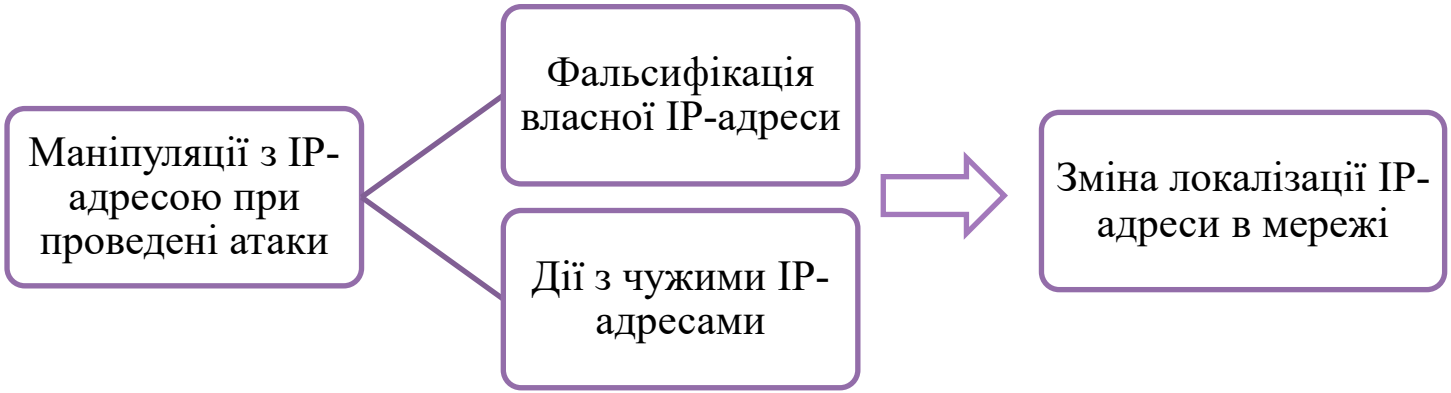


IP-адреса – це адреса, що ідентифікує комп'ютер в мережі.



Види атак:

- TCP flooding
- UDP flooding
- IP-спуфінг (IP Spoofing)
- Атака Smurf (Smurf attack)
- «Перехоплення маршруту» (IP hijacking)
- Атака передбачення номера послідовності TCP



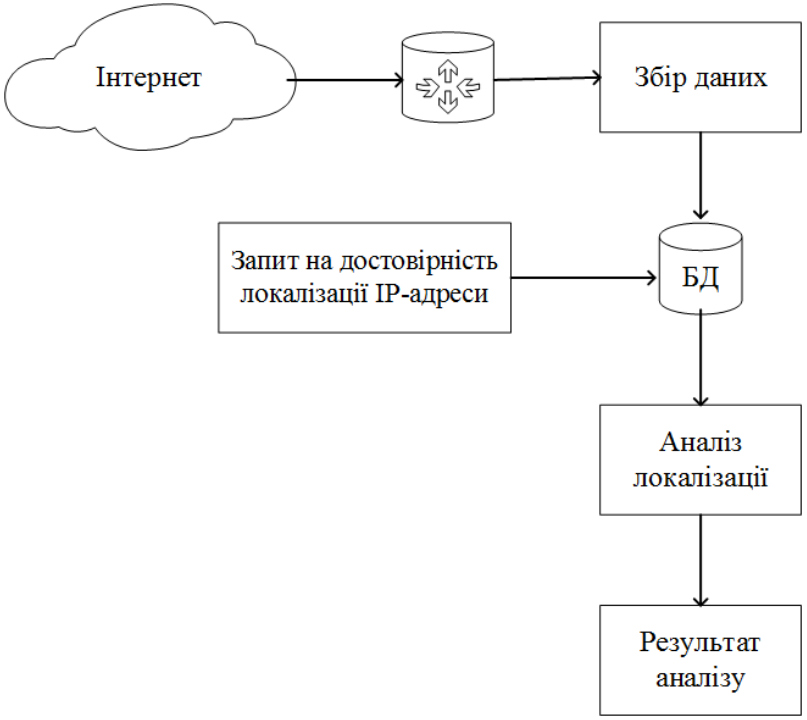
Методи визначення локалізацій IP-адрес:

- Офіційний запит до провайдера;
- Пошук по даним WHOIS;
- Пошук за допомогою ГЕО-IP інструменту.

Недоліки методів визначення локалізацій IP-адрес:

- Відносно низька швидкість отримання результатів;
- Висока ймовірність невірного визначення локалізації;
- Повільне оновлення баз даних;
- Визначення локалізації лише за кінцевою точкою IP-маршруту.

Схема принципу роботи програми



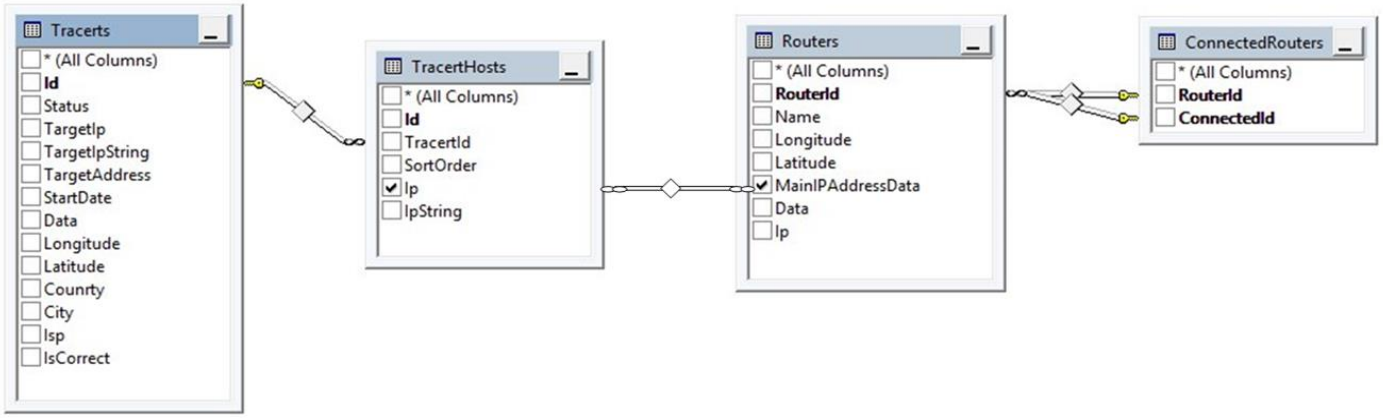
Завдання, які необхідно вирішити для роботи програми:

- Організація збору даних
- Аналізування локалізацій
- Інтерфейс взаємодії з користувачем

Організація збору даних :

- Створення бази даних з інформацією про маршрутизатори, їх зв’язки та маршрути;
- Розробка та реалізація програмного модуля для роботи з базою даних.

Вигляд діаграма бази даних в програмному середовищі



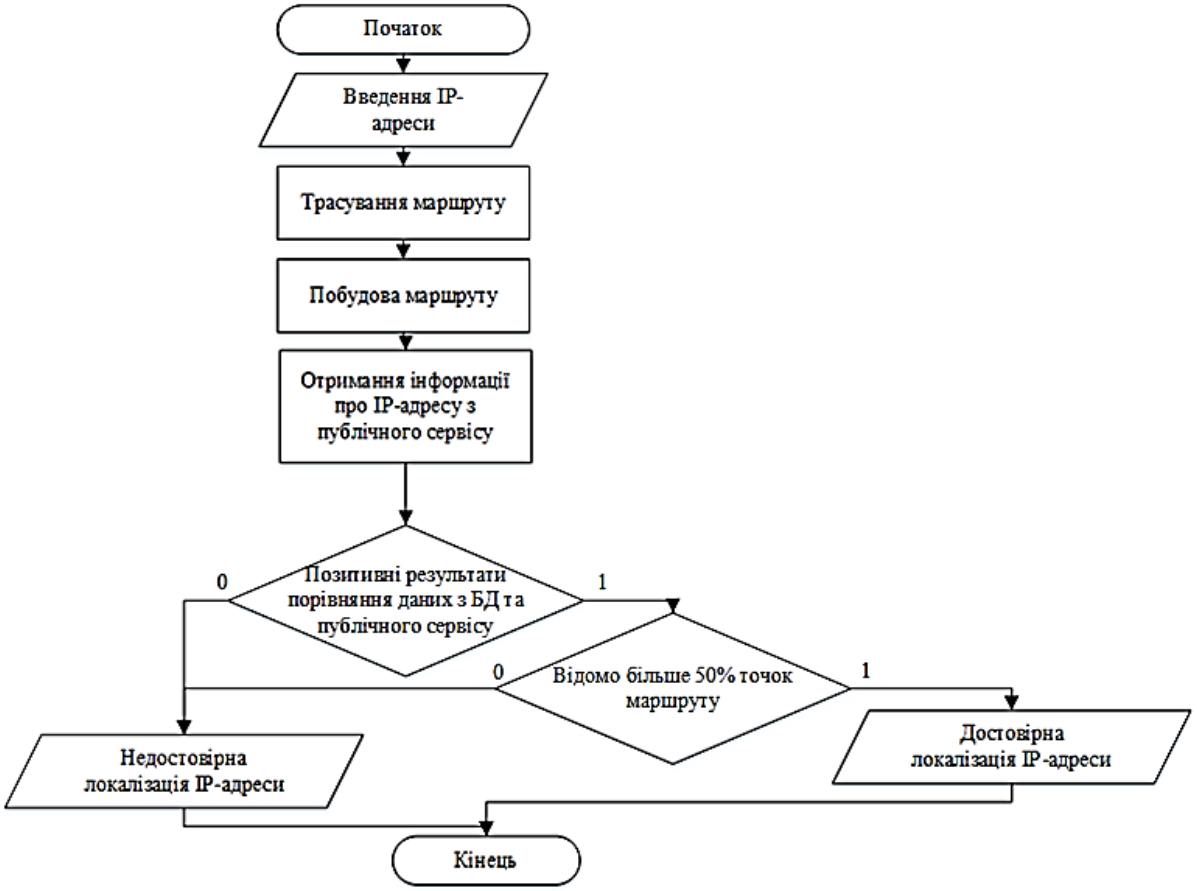
Програмний модуль виконує збір даних до БД за допомогою команди трасування маршруту traceroute

Вигляд заповненої таблиці «Routers»

RouterId	Name	Longitude	Latitude	MainIPAddressData	Data	Ip
A36A14...	AS13032 Kyiv National T...	30,5167	50,4333	3548498523	{"as":"AS130...	91.202.129....
0D5B19...	AS42896 TOV Research ...	34,1108	44,9572	434971073	{"as":"AS428...	193.33.237.25
EA0691...	AS47898 PAN-Telecom ...	30,5234	50,4501	33146459	{"as":"AS478...	91.198.249.1
5EA9F0...	AS197175 Teleradiokom...	33,6876	46,1141	222880091	{"as":"AS197...	91.225.72.13
08E8B1...	AS15772 Kyiv, Ukraine	30,5066	50,4481	834475225	{"as":"AS157...	217.20.189.49
B59BFF...		30,5234	50,4501	2201878969	{"as":"","city"...	185.1.62.131
8F38591...	AS33871 Norilsk-Teleco...	88,2206	69,3406	2580562768	{"as":"AS338...	80.67.208.153
8AF5E4...	AS31546 NORMA TELE...	28,8148	47,006	649334303	{"as":"AS315...	31.14.180.38
0EDAF0...	AS1257 TELE2	11,9746	57,7089	995095682	{"as":"AS125...	130.244.79.59

Модуль-аналізатор локалізацій IP-адрес

Схема роботи модуля-аналізатора локалізацій



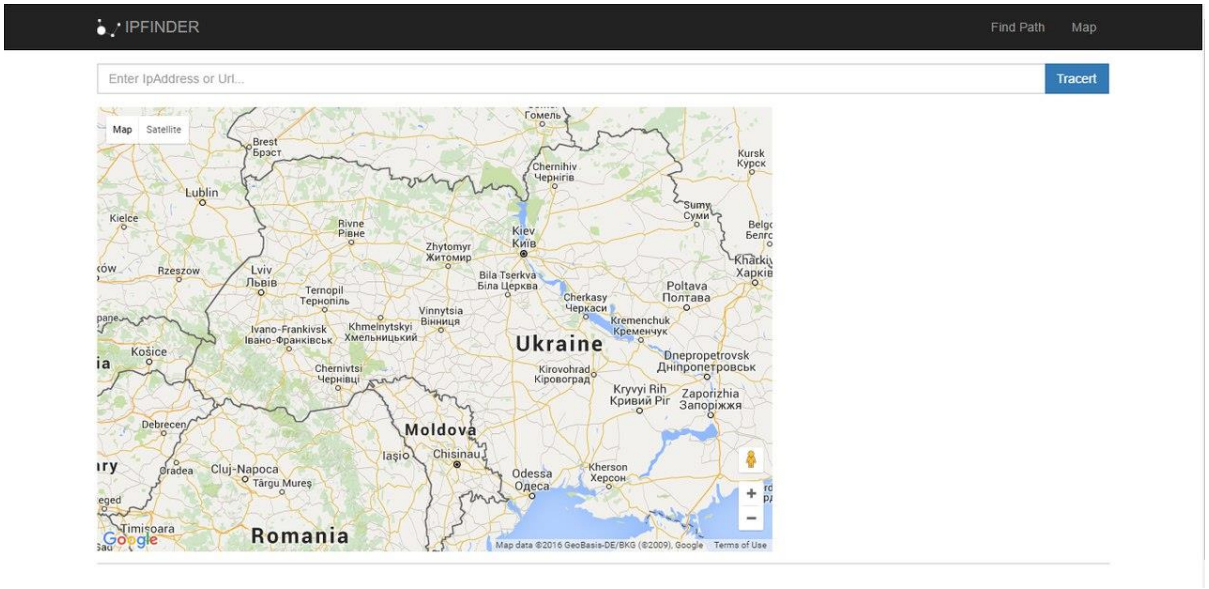
Фрагмент заповненої таблиці «Tracert» після проведення аналізу

IsCorrect	Status	TargetIp	TargetIpString	TargetAddress	StartDate	Data	Longitude	Latitude
-1	0	197926337	193.29.204.11	193.29.204.11	2016-06-03 22:48:18.1500000	{"as":"AS21096 De...	30,5167	50,4333
-1	0	197926337	193.29.204.11	193.29.204.11	2016-06-03 22:39:25.0270000	{"as":"AS21096 De...	30,5167	50,4333
1	0	134744072	8.8.8.8	8.8.8.8	2016-06-04 13:08:21.0330000	{"as":"AS15169 Go...	-122,0838	37,386

Розробка користувацького інтерфейсу

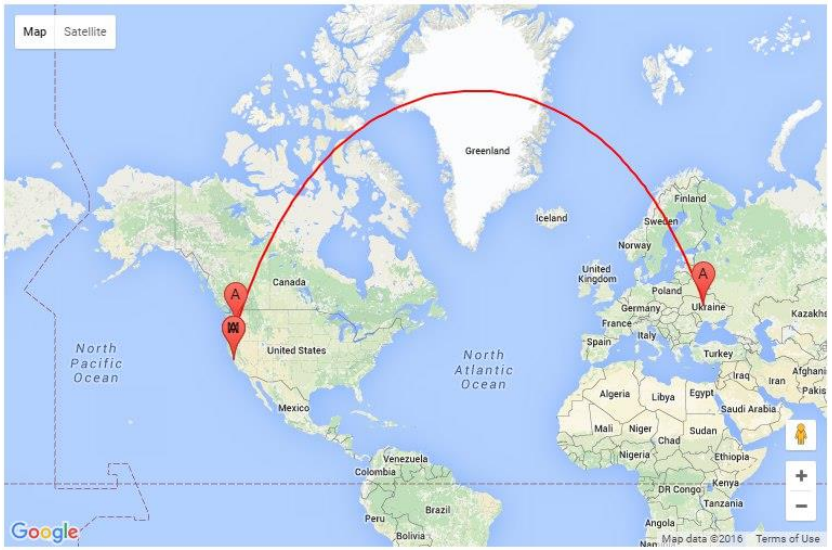
Вигляд головної сторінки веб-додатку

Вигляд сторінки проведення аналізу



Тестування роботи програми

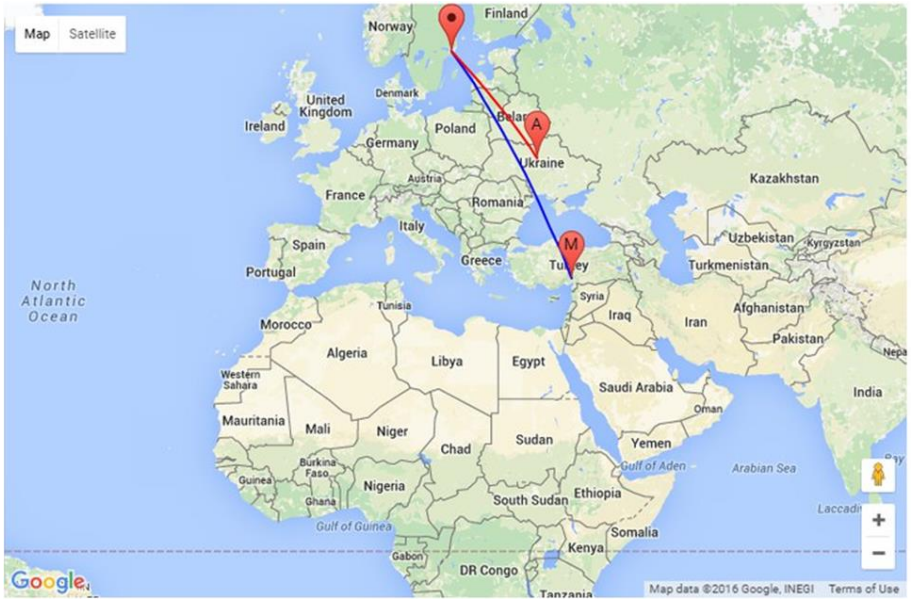
IP-адреса з завідомо достовірною локалізацією IP-адреси



8.8.8.8 - Finished: IpAddress is correct

1. 192.168.0.1 - Finished: IpAddress is correct
2. 192.168.1.1 - Finished: IpAddress is correct
3. 195.5.5.186 - Finished: IpAddress is correct
   As: AS6849 PJSC UKRTELECOM
   Isp: PJSC Ukrtelecom
   Counrty: Ukraine
   City: Ukrainka
   Longitude: 30,7435
   Latitude: 50,1531
4. 10.80.40.22 - Finished: IpAddress is correct
5. 74.125.52.238 - Finished: IpAddress is correct
   As: AS15169 Google Inc.
   Isp: Google
   Counrty: United States
   City: The Dalles
   Longitude: -121,1543

IP-адреса з завідомо недостовірною локалізацією IP-адреси



95.173.183.51 - Finished: IpAddress is incorrect

1. 192.168.0.1
2. 192.168.1.1
3. 195.5.5.186
   As: AS6849 PJSC UKRTELECOM
   Isp: PJSC Ukrtelecom
   Counrty: Ukraine
   City: Ukrainka
   Longitude: 30,7435
   Latitude: 50,1531
4. 10.50.19.10
5. 213.248.92.113
   As:
   Isp: TeliaSonera AB
   Counrty: Sweden
   City: Stockholm (Farsta)
   Longitude: 18,0903
   Latitude: 59,2445

Дякую за увагу!