

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ВНУТРІШНІХ СПРАВ**

*кафедра кібербезпеки та DATA-технологій, факультет № 6*

# **МЕТОДИЧНІ МАТЕРІАЛИ**

## **до практичних занять**

**з навчальної дисципліни**

**Аналітична робота під час протидії  
кіберзлочинності**

**вибіркових компонент освітньої програми першого рівня вищої освіти  
125 Кібербезпека (безпека інформаційних та комунікаційних систем)**

**Харків 2023**

## **ЗАТВЕРДЖЕНО**

Науково-методичною радою  
Харківського національного  
університету внутрішніх справ  
Протокол від 30.08.2023 № 7

## **СХВАЛЕНО**

Вченою радою факультету № 6  
Протокол від 25.08.2023 № 7

## **ПОГОДЖЕНО**

Секцією Науково-методичної ради  
ХНУВС з технічних дисциплін  
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій (*протокол від 15.08.2023 № 8*)

### **Розробник:**

Доцент кафедри кібербезпеки та DATA-технологій, к.ю.н., професор Манжай О.В.

### **Рецензенти:**

Тулупов В.В., доцент кафедри кібербезпеки та DATA-технологій факультету № 6  
Харківського національного університету внутрішніх справ к.т.н., доцент;

Павликівський В.І., перший проректор Харківського університету, д.ю.н., професор

## ЗМІСТ

1. Розподіл часу навчальної дисципліни за темами.....	4
2. Методичні вказівки до практичного навчання .....	5
Практичне заняття. Моделі стримування злочинності .....	5
Практичне заняття. Застосування методології ANACAPA у протидії злочинності .....	7
Практичне заняття. Пошук інформації про об'єкти в мережі .....	8
Практичне заняття. Програмні засоби кримінального аналізу .....	13
3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті.....	18

# 1. Розподіл часу навчальної дисципліни за темами

## Денна форма навчання

## Денна форма навчання

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Вид контролю	
	Всього	з них:					
		лекцій	Семінарські заняття	Практичні заняття	Лабораторні заняття		Самостійна робота
Семестр № 7							
Тема № 1 Основні поняття та моделі стримування злочинності	26	4		2	0	20	Екзамен
Тема № 2 Поняття та зміст кримінальної розвідки (зарубіжний досвід)	30	4		2	4	20	
Тема № 3 Розвідка з відкритих джерел (OSINT)	30	4		4	4	18	
Тема № 4 Програмні інструменти кримінальної розвідки	34	4		2	8	20	
Всього за семестр № 8:	120	16		10	16	78	

## Заочна форма навчання

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		лекцій	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 7							
Тема № 1 Основні поняття та моделі стримування злочинності	28	2		2		24	Екзамен
Тема № 2 Поняття та зміст кримінальної розвідки (зарубіжний досвід)	32	2		2	4	24	
Тема № 3 Розвідка з відкритих джерел (OSINT)	30	2		2	2	24	
Тема № 4 Програмні інструменти кримінальної розвідки	30	2			2	26	
Всього за семестр № 8:	120	8		6	8	98	

## 2. Методичні вказівки до практичного навчання

### Тема № 1 Основні поняття та моделі стримування злочинності

#### Практичне заняття. Моделі стримування злочинності

Навчальна мета заняття: провести гру «Дебати» за темою для виявлення та закріплення знань.

Час проведення \*<sup>1</sup> год. Місце проведення: навчальна аудиторія.  
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Устаткування: ручка, зошит.

#### Порядок проведення заняття

1. Студенти (слухачі) заздалегідь отримують перелік питань для підготовки (див. у кожній лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обох командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.  
Критерії оцінювання (за п'ятибальною шкалою кожний):  
- повнота та аргументованість відповідей;  
- робота в команді;  
- дотримання правил етикету;
12. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
13. По закінченні гри підбиваються підсумки.

#### *Література, методичне та матеріально-технічне забезпечення занять*

1. Wang Liang & Zhao Jihong Solomon Contemporary police strategies of crime control in U.S. and China: a comparative study. *Crime, Law and Social Change*. 2016. № 5(66). pp. 525-537.

<sup>1</sup> Час проведення заняття визначається згідно з програмою

2. Tayebi M. A. Glässer U. *Social Network Analysis in Predictive Policing: Concepts, Models and Methods*. Springer, 2016. 133 p. (DOI 10.1007/978-3-319-41492-8)
3. Орлов Ю. Ю. Застосування сучасної методики прогнозування та запобігання злочинам у поліції США // *Кримінальна розвідка: методологія, законодавство, зарубіжний досвід : матеріали Міжнар. наук.-практ. конф., м. Одеса, 29 квітня 2016 р. Одеса : ОДУВС, 2016. 184 с. С. 22-24.*
4. Водько Н. П. О содержании термина «криминальная разведка». *Південноукраїнський правничий часопис*. 2016. № 1. С. 83-85.
5. Moreto W.D., Cowan D., Burton C. Towards an Intelligence-Led Approach to Address Wildlife Crime in Uganda. *Policing: A Journal of Policy and Practice*. 2017. № pax064. (doi.org/10.1093/police/pax064).
6. Strang S. J. Network Analysis in Criminal Intelligence. A. J. Masys (ed.), *Networks and Network Analysis for Defence and Security*, Lecture Notes in Social Networks. 2014. P. 2-26. DOI: 10.1007/978-3-319-04147-6\_1.
7. Албул С. В., Користін О. Є. Концепція розвитку кримінальної розвідки органів внутрішніх справ України. *Південноукраїнський правничий часопис*. 2015. № 1. С. 158-163.
8. Манжай О. В., Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic National: Teorie si Practică*. 2015. № 3(13). С. 100-105.
9. Potparič Damjan, Dvoršek Anton Critical Success Factors in Establishing a National Criminal Intelligence Model in Slovenia // *Policing in central and eastern Europe – social control of unconventional deviance : conference proceedings, [Ljubljana, Slovenia, 22-24 September 2010] / editors Gorazd Meško, Andrej Sotlar and John Winterdyk ; [drawings Philip Spence]. Ljubljana : Faculty of Criminal Justice and Security, 2011. pp. 259-282.*
10. Estévez E. E. Reformando la inteligencia policial en la provincia de Buenos Aires. *Policing and Society: Revista Latinoamericana de Estudios de Seguridad*. № 15. 2014. pp. 71-84.

## Тема № 2 Поняття та зміст кримінальної розвідки (зарубіжний досвід)

### Практичне заняття. Застосування методології ANACAPA у протидії злочинності

Навчальна мета заняття: відпрацювати навички аналізу надходжуваної інформації.

Час проведення     \*<sup>1</sup> год    . Місце проведення: навчальна аудиторія.  
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

*Вхідні дані (адаптовано з навчальної практики для британських поліцейських):*

1. Дані з протоколу допиту свідка 01/22: Петренко на поставлене слідчим запитання розповів, що із Москаленко їх познайомив Заліско, який представив Москаленко як фахівця у сфері зниження оподаткування та брокерських послуг. Також у рамках спілкування Москаленко відзначив, що його неофіційним партнером по бізнесу є Лоботенко. [В-2].

2. Відомості з реєстру юридичних осіб 05/22: Уткін ідентифікований як директор, а Лоботенко як експедитор компанії «Ліхтарик», що спеціалізується на перевезеннях та наданні фінансових послуг. ТОВ «Ліхтарик» податкового боргу не має. Задекларований дохід за останній рік складає 321 тис. грн [А-1].

3. Протокол огляду вилученого відеозапису з камери спостереження в таксі та відеореєстратора 06/22: 12 вересня поточного року о 01:12 Лоботенко та Саєнко здійснювали переміщення в таксі з адреси вул. Куліка, 12 до магазину «Теремок» за адресою вул. Лютого, 7. За цією ж адресою розташовано ТОВ «Шоколад». Запис камери відеореєстратора засвідчує, що після виходу з таксі Лоботенко та Саєнко увійшли до дверей із написом ТОВ «Шоколад». Під час руху в таксі Лоботенко емоційно доводив Саєнку, що він є найбільшим постачальником героїну з території Афганістану у регіоні свого проживання [А-1].

4. Відомості з Інформаційного порталу Національної поліції України 18/22: три роки тому Саєнко і Ракітін були разом затримані за незаконне зберігання та перевезення наркотичних засобів без мети збуту біля складу логістичної компанії «Аврора».

5. Відомості з Єдиного державного реєстру судових рішень 19/22: Директор ТОВ «Аврора» Заліско виступав свідком сторони захисту у провадженні про незаконне зберігання та перевезення наркотичних засобів Саєнком і Ракітіним. Адвокатом підсудних був Алевтян, який також є штатним юристом ТОВ «Аврора» [А-1].

6. Відомості з матеріалів журналістського розслідування сайту «Кабачок» 20/22: Голко і його компанія «Голко і партнери» займається незаконною легалізацією доходів та пов'язана з організованими злочинними угрупованнями, які займаються наркобізнесом [В-2].

7. Відомості з реєстру фіскальної служби 05/22: Компанія «Ліхтарик» є клієнтом компанії «Голко і партнери» [А-1].

8. Відомості з аналітичної довідки за результатами моніторингу інформації з відкритих джерел 25/22: Уткін через підставних осіб є фактичним володільцем компанії «Колобок». Компанія «Колобок» спеціалізується на імпорті фруктів та фігурувала в матеріалах розслідувань щодо незаконного постачання наркотичних засобів в Україну два рази за останні шість років [В-2].

### Порядок проведення заняття

1. Групу розділяють на три команди.
2. Кожна команда виконує наступні завдання:
  - побудувати матрицю асоціацій та дерево зв'язків. Сформулювати аналітичний висновок.
  - сформулювати власні вхідні дані щодо ситуації, пов'язаної з кіберзлочином.
  - команди обмінюються завданнями;
  - відповідно до нових вхідних даних кожна команда будує матрицю асоціацій та дерево зв'язків, готує аналітичний висновок.
3. Підбиваються підсумки.

<sup>1</sup> Час проведення заняття визначається згідно з програмою

### ***Література, методичне та матеріально-технічне забезпечення занять***

1. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 с.
2. Манжай О. В. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням / О. В. Манжай, Є. О. Жицький // Jurnalul Juridic National: Teorie si Practică. – 2015. – № 3(13). – С. 100-105.
3. Carter J. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory / J. G. Carter, S. W. Phillips, S. M. Gayadeen // Journal of Criminal Justice. – 2014. – № 42. – Р. 433-442.

## **Тема № 3 Розвідка з відкритих джерел (OSINT)**

### **Практичне заняття. Пошук інформації про об'єкти в мережі**

Навчальна мета заняття: отримати практичні навички пошуку інформації про осіб шляхом використання кіберпростору.

Час проведення     \*<sup>1</sup> год    . Місце проведення: комп'ютерний клас.  
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгфонний кабінет)

**Устаткування:** персональний комп'ютер (ПК) зі встановленою операційною системою Windows 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

В процесі документування нерідко доводиться здійснювати пошук інформації про об'єкти, пов'язані зі злочиним, в мережі. Для цього можуть бути використані можливості інформаційно-пошукових систем, соціальних мереж, локальних баз даних тощо.

В процесі пошуку засобами пошукових систем корисним буде знання спеціалізованих операторів, з якими можна ознайомитись на офіційних сайтах інформаційно-пошукових систем. Зазвичай, базові оператори є однаковими в усіх цих системах. Наприклад, фраза в лапках, введена у пошуковому вікні Google та Яндекс, означатиме пошук фрази цілком.

Якщо потрібно дізнатися, де зустрічається логін до електронної пошти, в Google можна скористатися запитом: "login \* ru|ua|com|net", у результаті виконання якого буде знайдено сторінки, у змісті яких зустрічається текст, який починається символами login та закінчується символами ru, ua, com або net.

У випадку, коли правоохоронець не повною мірою володіє мовою спеціальних запитів в інформаційно-пошукових системах, йому буде корисною функція розширеного пошуку:

- Google: Налаштування → Розширений пошук;

- Яндекс: значок  у вікні пошуку.

Серед *корисних ресурсів* для пошуку слід виділити:

- findface.ru для встановлення особи за фотографією;
- агрегатор інформації з соціальних мереж [www.radaris.com](http://www.radaris.com);
- набір інструментів для збирання інформації з відкритих джерел [osintframework.com](http://osintframework.com), [inteltechniques.com](http://inteltechniques.com);
- агрегатор інформації про юридичних осіб [youcontrol.com.ua](http://youcontrol.com.ua), [iplex.com.ua/](http://iplex.com.ua/);
- пошук у базах даних кадрових агентств (наприклад, [work.ua](http://work.ua));
- пошук у сервісах телефонних номерів ([www.truecaller.com](http://www.truecaller.com), [sync.me](http://sync.me), [findnumberapp.com](http://findnumberapp.com));
- сервіс пошуку розташування точок доступу Wi-Fi за MAC-адресою або назвою (для пошуку потрібно зареєструватись) [wagle.net](http://wagle.net);
- боти (наприклад, для Telegram: @OpenDataUABot, @e007bot, @OpenDeclarationBot, @d\_TarasBotagent);
- пошук осіб за контекстом ([pipl.com/api/demo](http://pipl.com/api/demo));

<sup>1</sup> Час проведення заняття визначається згідно з програмою



- пошук у базах втрачених паролів (застосування <https://github.com/D4Vinci/Cr3dOv3r>);
- банківські сервіси переказів (наприклад, Ощад24/7 → Переказ за номером телефону).

Вхідні дані.

Таблиця 1. Оператори Google

Оператори	Значення	Приклад
«»	Пошук точної фрази або словосполучення.	«торгівля людьми»
«слово*слово»	Пропущено слово у виразі	«надання * послуг»
(логічне АБО)	Пошук будь-якого зі слів	виставки   експозиції
& (логічне І)	Слова в межах одного речення	дитяче&порно
()	Дужки формують групи у складних запитах	(Інтим   Україна) & (Київ   Буча)
-	Вилучення слова з пошуку або сторінки	Київ -site:ttt.org
/ N	Відстань слова в будь-який бік	робота /2 стриптиз
/ + N і /-N	Точна відстань між словами	Іван /-1 Іванов
+	Слова, які обов'язково повинні бути присутніми в результатах пошуку	інтим + робота + Ізраїль
_	Зв'язування двох слів.	швидкий заробіток
..	Пошук цифр у заданому діапазоні	\$50..\$100
@	Пошук електронної пошти	@googler
site:	Пошук в структурі одного (заданого) сайту, домену.	site:trefdfd.ua
link:	Пошук сторінок, що містять посилання на сторінку зазначену в запиті.	link:www.unian.net
inurl:	Пошук слова в рядку адреси сторінки	inurl:xxx
allinurl:	Пошук всіх слів в рядку адреси сторінки	allinurl:xxx
define:	Визначення слова, словосполучення	define:органи
filetype:	Пошук за типами файлів	діти filetype:jpg
related:	Схожі сторінки на зазначену	related:www.serdsf.net
info:	Інформація Google про сторінку зазначену у запиті	info:www.sxfsdcv.ua
intitle:	Пошук в заголовках сторінок	intitle:проститутки
allintitle:	Пошук всіх слів у заголовках	allintitle:робота на півночі
cache:	Попередні версії сторінок, сайтів	cache:www.adsdadasd.com
numrange:	Результати по вказаній даті (проміжку дат)	Іванова numrange:1997-1998

Таблиця 2. Шаблон пошуку

№ з/п	Критерій	Ознака	Значення	Джерело
1.	Загальна інформація про особу (питання «Хто?»)	Прізвище, ім'я та по батькові		
		Стать		
		Вік (зокрема, дата народження)		
		Раса / національність / віросповідання		
		Соціальне походження		
		Освіта		
		Професія		
		Посада		

№ з/п	Критерій	Ознака	Значення	Джерело
		Майновий стан		
		Ідентифікаційні коди		
		Фізичні характеристики (група крові, зріст), стан здоров'я		
		Членство в організаціях, партіях, громадських об'єднаннях тощо		
		Громадянство		
		Псевдоніми (ніки)		
		Імена користувачів		
		Паролі		
2.	<b>Географічні дані / Місце розташування</b> (питання «Де?» та «Як знайти?»)	Місце народження		
		Домашня адреса (місце реєстрації, місце фактичного проживання)		
		Телефонний номер (проводова лінія)		
		Поштова адреса		
		Кабельне телебачення		
		Мобільний телефон		
		Транспортний засіб та інше рухоме майно		
		Місця частого перебування (клуби, бари тощо)		
		Мережна адреса		
		Адреса електронної пошти		
		Персональний сайт		
		Профілі електронних ресурсів (електронний щоденник, профіль в соціальних мережах, на форумах тощо)		
		Номери мережних пейджерів (ICQ, IRC, Jabber, Odigo, MSN тощо)		
		Номери для конференц зв'язку з використанням Інтернет		
		Точка доступу для безпроводового комп'ютерного зв'язку		
3.	<b>Часові характеристики</b> (питання «Коли?»)	Дата і час певної події		
4.	<b>Зв'язки</b> (питання «З ким?»)	Члени сім'ї (в тому числі одружені та розлучені)		
		Інші соціальні зв'язки: співмешканці, друзі, партнери тощо		
		Контакти в певних місцях (зокрема, в кіберпросторі) або за місцем проживання (зокрема, сусіди).		
5.	<b>Сфера інтересів</b> (питання «Чим цікавиться?»)	Транспортні засоби		
		Зброя		
		Тварини		
		Техніка		
		Мистецтво		
		Колекціонування		
		Контрабанда		
		Землі, будівлі, бізнес-структури		

№ з/п	Критерій	Ознака	Значення	Джерело
6.	<b>Фактичні обставини</b> (питання «Що відбулося?»)	Спілкування		
		Факт використання певних засобів (комп'ютер, телефон) для створення, відправлення або отримання інформації (перегляд поштових даних, даних GPS тощо)		
		Економічні відносини: купівля, продаж, операції з кредитними картками тощо		
		Історія зайнятості (пошук та пропозиція роботи)		
		Протиправні дії (правопорушення, злочини)		
7.	<b>Системна характеристика</b> (питання «Яка особа?»)	Громадянська позиція		
		Професійні якості		
		Державна служба		
		Відгуки колективу		
		Результати тестувань (медичного, професійного, психологічного)		
		Самохарактеристика		
		Показники кредитоспроможності		
		Страхові рейтинги		

### Корисні ресурси

Мережні сховища	<a href="https://www.dropbox.com">https://www.dropbox.com</a> , — <a href="https://drive.google.com">https://drive.google.com</a> , <a href="https://mega.co.nz">https://mega.co.nz</a> , <a href="http://www.ge.tt">http://www.ge.tt</a>
Перелік існуючих безкоштовних VPN-мереж	<a href="http://www.makeuseof.com/tag/7-completely-free-vpn-services-protect-privacy">http://www.makeuseof.com/tag/7-completely-free-vpn-services-protect-privacy</a> — <a href="http://www.cachedpages.com/">http://www.cachedpages.com/</a>
Пошук видалених сторінок	— <a href="http://www.archive.org/">http://www.archive.org/</a>
Пошук завантажень з визначеної IP-адреси	<a href="https://iknowwhatyoudownload.com/ru/peer/">https://iknowwhatyoudownload.com/ru/peer/</a> — <a href="http://www.nomer.org">http://www.nomer.org</a> , — <a href="http://www.radaris.com">http://www.radaris.com</a> <a href="http://lookup.com">http://lookup.com</a> <a href="https://www.imena.ua/blog/ukraine-database/">https://www.imena.ua/blog/ukraine-database/</a> <a href="http://osintframework.com/">http://osintframework.com/</a> <a href="https://youcontrol.com.ua">https://youcontrol.com.ua</a> <a href="http://findmobil.info/">http://findmobil.info/</a>
Пошук зображення особи	<a href="https://images.google.com/imghp?tbm=isch&amp;tbs=itp:fface&amp;gws_rd=ssl">https://images.google.com/imghp?tbm=isch&amp;tbs=itp:fface&amp;gws_rd=ssl</a> — <a href="http://www.findbyface.com">http://www.findbyface.com</a>
Пошук за зображенням	— <a href="http://www.findbyface.com">http://www.findbyface.com</a>
Пошук зображень (копій)	<a href="http://images.google.com">http://images.google.com</a> , — <a href="http://images.search.yahoo.com">http://images.search.yahoo.com</a> , <a href="http://www.tineye.com">http://www.tineye.com</a> ,
Пошук по онлайн щоденниках	<a href="http://tumblr.com">http://tumblr.com</a>

Пошук по профілях Google+	—	<a href="http://google.com/profiles">http://google.com/profiles</a>
Пошук по сервісах обміну фотографіями і відеозаписами	—	<a href="http://www.youtube.com">http://www.youtube.com</a> , <a href="http://instagram.com">http://instagram.com</a> , <a href="http://flickr.com">http://flickr.com</a> , <a href="http://picasa.google.com">http://picasa.google.com</a>
Пошук серед осіб, які поступали у вищі навчальні заклади України	—	<a href="http://vstup.info">http://vstup.info</a>
Сервіси для збирання інформації про електронні ресурси за адресами	—	<a href="http://robtex.com">http://robtex.com</a> , <a href="http://he.net">http://he.net</a>
Соціальні мережі	—	<a href="http://facebook.com">http://facebook.com</a> , <a href="http://instagram.com">http://instagram.com</a> , <a href="http://twitter.com">http://twitter.com</a>
WEB-архіви	—	<a href="http://archive.is/">http://archive.is/</a> , <a href="http://archive.org/">http://archive.org/</a>
Пошук розташування точок доступу Wi-Fi за MAC-адресою або назвою (для пошуку потрібно зареєструватись)	—	<a href="https://www.wigle.net/">https://www.wigle.net/</a>
Фішингові сайти	—	<a href="https://ema.com.ua/report-an-incident/black-list/">https://ema.com.ua/report-an-incident/black-list/</a>

1. Здійснити пошук даних будь-якої відомої особи за її електронною поштою та мережним псевдонімом або іншими первинними даними.
2. Систематизувати знайдені відомості, у якості шаблону взяти перелік ідентифікаторів особи. Для пошуку використовувати матеріали з теоретичних відомостей.
3. Зібрати інформацію вказану викладачем за фотознімком.

### ***Література, методичне та матеріально-технічне забезпечення занять***

1. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. – К., 2017. – 148 с.

## Тема № 4 Програмні інструменти кримінальної розвідки

### Практичне заняття. Програмні засоби кримінального аналізу

Навчальна мета заняття: ознайомитися з роботою програмних пакетів Maltego та i2.

Час проведення \_\_\*<sup>1</sup> год\_\_. Місце проведення: комп'ютерний клас.  
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

**Устаткування:** персональний комп'ютер (ПК) зі встановленою операційною системою Windows XP або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Сучасна правоохоронна діяльність характеризується необхідністю обробки та аналізу великих масивів даних. Нерідко доводиться обробляти дані телефонного білінгу правопорушників, файли протоколів відповідних транзакцій та активності в мережі Інтернет. З цією метою може бути використано спеціалізоване програмне забезпечення. У якості прикладів в даному контексті можна назвати Datasplloit, i2, Maltego, Splunk. Система Datasplloit (<https://github.com/upgoingstar/datasplloit>) буде корисною для збирання та аналізу інформації про домен, електронну пошту тощо, Splunk (<https://www.splunk.com>) – для збирання та аналізу машинних даних, наприклад, лог-файлів. Програма Maltego у безкоштовному виконанні (<https://www.paterva.com/>) цілком може бути застосована для роботи з невеликим обсягом даних, у той час як i2 ([www.ibm.com/software/products/ru/analysts-notebook](http://www.ibm.com/software/products/ru/analysts-notebook)) орієнтована на роботу з так званими «big data».

Окремо хотілося б звернути увагу на розроблену за участі працівників ГУНП України в Харківській області систему RICAS (Real-time Intelligence Crime Analytics System), з використанням якої можливо розкрити окремі злочини, навіть не виходячи з кабінету ([police.kh.ua](http://police.kh.ua)).

Розглянемо на прикладі роботу застосувань Maltego та i2.

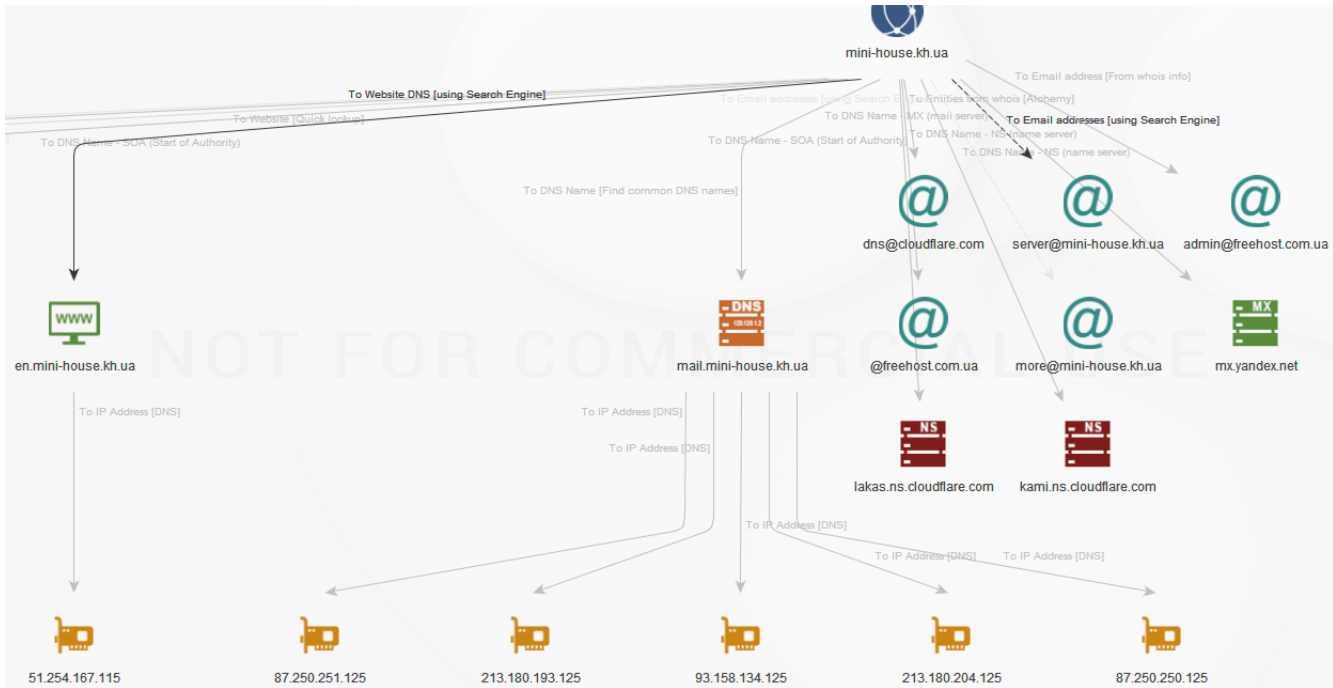
#### **Maltego**

Програма Maltego має декілька версій. Серед них варто звернути увагу на умовно-безкоштовні Maltego CE та Maltego CaseFile. Перша призначена для аналізу даних онлайн, друга – для роботи з локальними файлами. Мова інтерфейсу програми – англійська.

Для використання означених версій Maltego їх потрібно завантажити з сайту виробника, після чого зареєструватися та авторизуватися у програмі.

Сам процес використання програми є доволі зрозумілим навіть пересічному користувачу. Спочатку потрібно обрати відповідну методику аналізу. Після одержання попереднього результату його можна деталізувати із застосуванням інших методів наведених у випадіючому списку в меню Run View. На рис. 1 наведено приклад аналізу за базовим методом Footprint L1 сайту [mini-house.kh.ua](http://mini-house.kh.ua) із наступним більш детальним аналізом на предмет наявності асоційованих з ним електронних поштових адрес та їх даних (зокрема методу To Email addresses [using Search Engine]). Вказаний аналіз проводився у програмі Maltego CE.

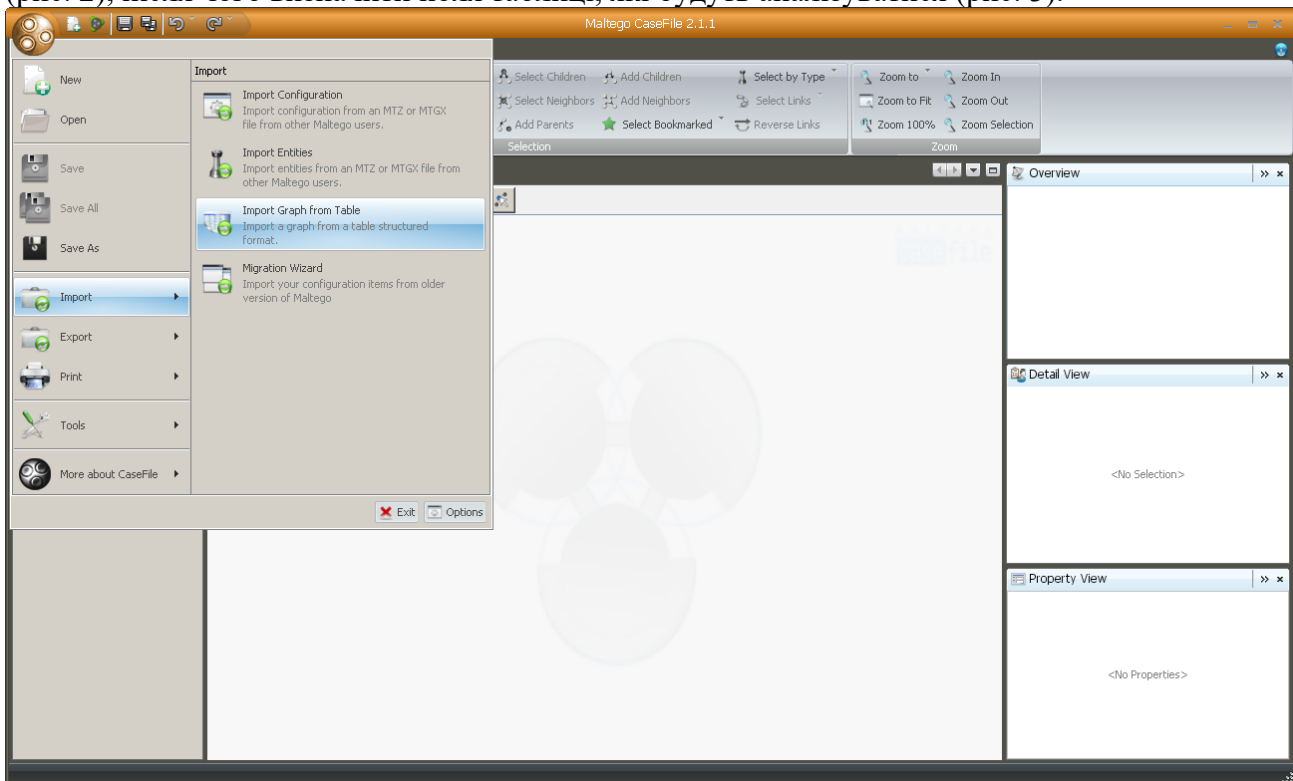
<sup>1</sup> Час проведення заняття визначається згідно з програмою



**Рис. 1. Результат аналізу сайту**

Якщо потрібно аналізувати дані з локальних файлів, можна скористатися програмою Maltego CaseFile.

Для імпорту відповідних даних слід у розділі Import обрати Import Graph from Table (рис. 2), після чого визначити поля таблиці, які будуть аналізуватися (рис. 3).



**Рис. 2. Імпорт локальних даних до програми Maltego CaseFile**

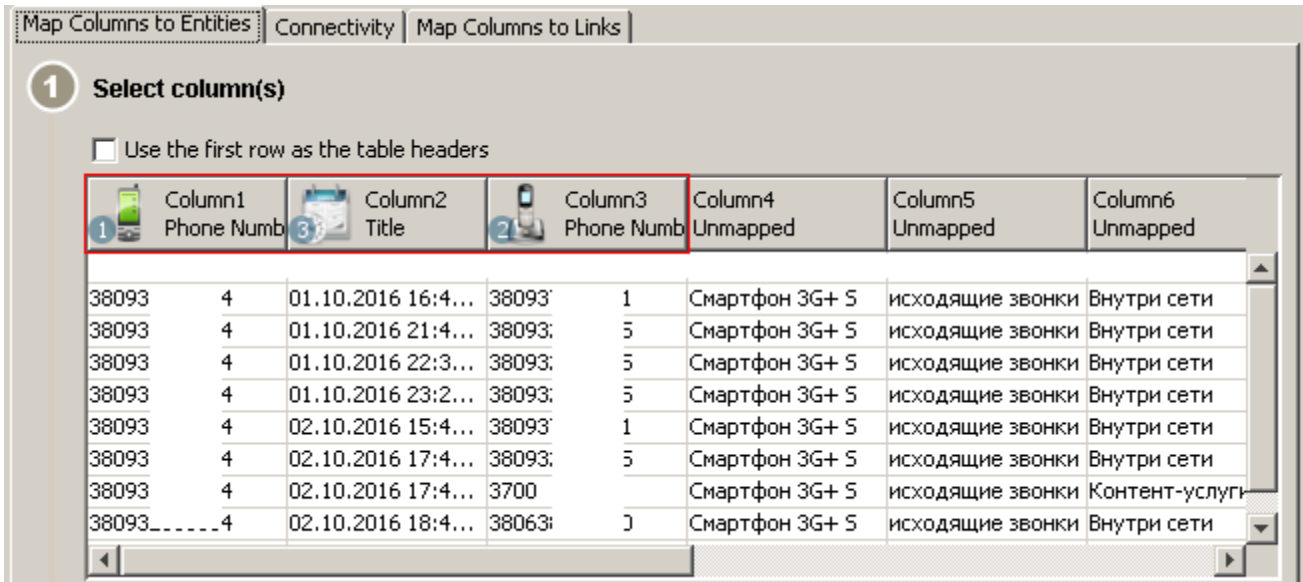


Рис. 3. Визначення даних для аналізу

У результаті аналізу одержуємо відповідний граф (рис. 4), форма якого може бути змінена.

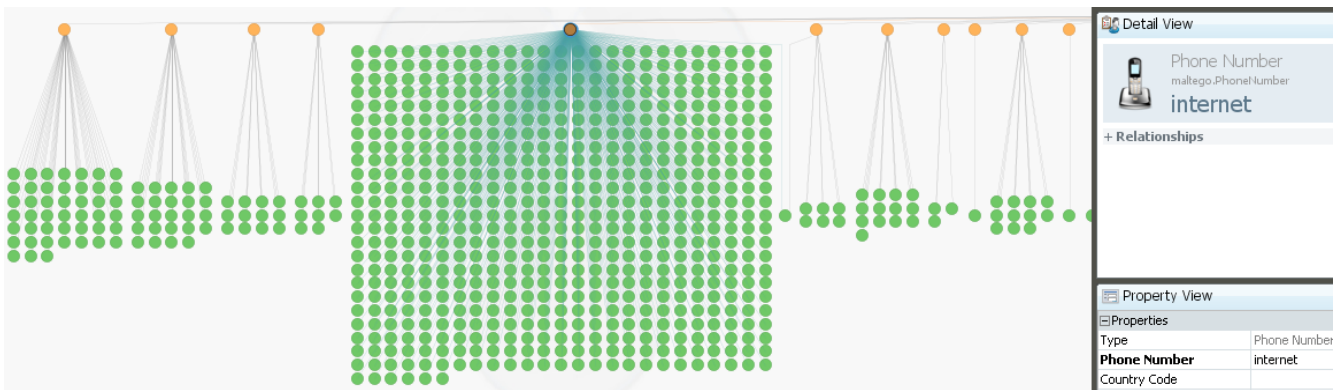
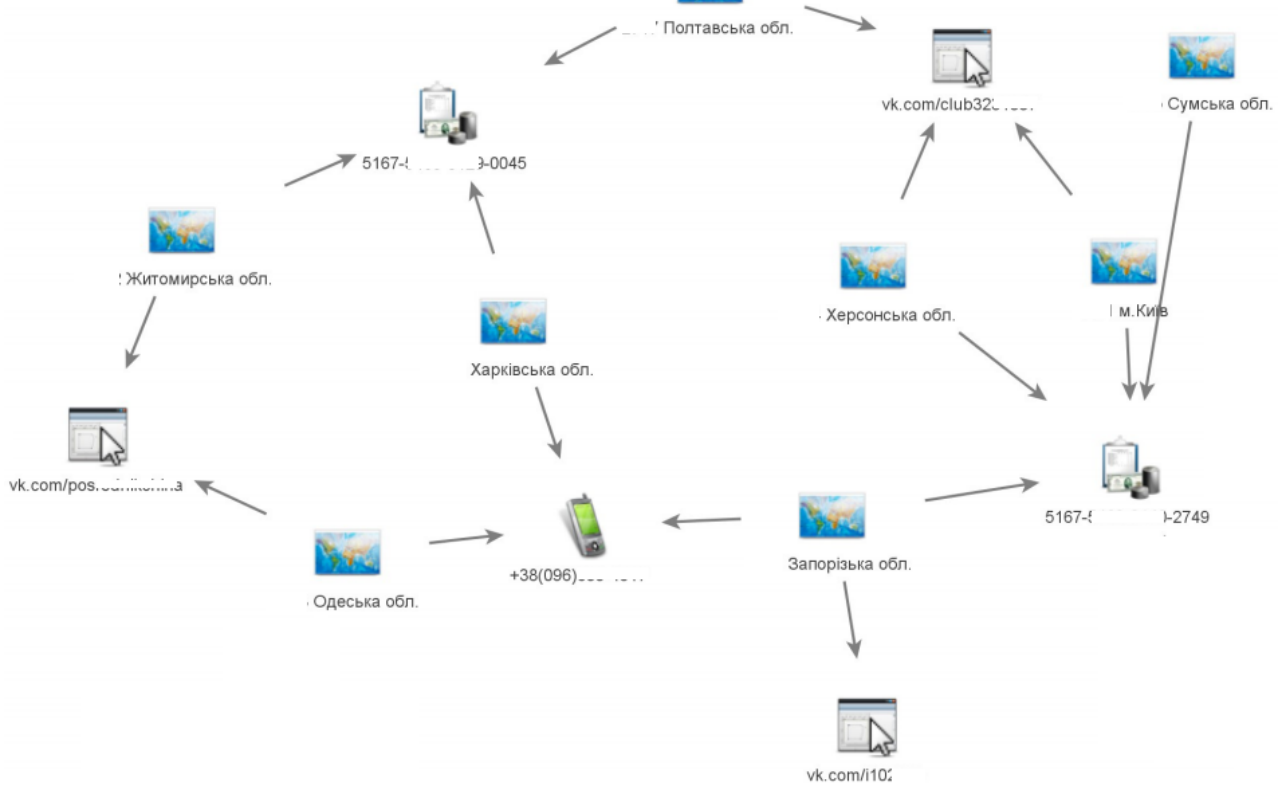


Рис. 4. Результати аналізу

У даному випадку на графіку жовтими точками позначено конкретний номер або назву послуги, а зеленим – дати та час, коли відбувалися відповідні дії. У випадку проведення реального аналізу самі дані для аналізу можна конкретизувати та змінювати, щоб у кінцевому випадку одержати більш візуально значущу інформацію про конкретну особу, подію або групу подій. На рис. 5, наприклад, наведено фрагмент діаграми аналізу шахрайської схеми, яка відбувалася з використанням мережі Інтернет.



**Рис. 5. Фрагмент діаграми**

Сформовані у програмі Maltego діаграми та інші результати аналізу можуть бути збережені у вигляді звітів.

## IBM i2

Для роботи з великим масивами даних вельми корисним представляється програмний комплекс IBM i2, зокрема IBM i2 Analyst's Notebook. Порядок роботи з даною програмою так само, як і у попередньо наведеному випадку, є візуально зрозумілим. Хоча велика кількість інструментів та налаштувань передбачає необхідність базових знань роботи з програмою.

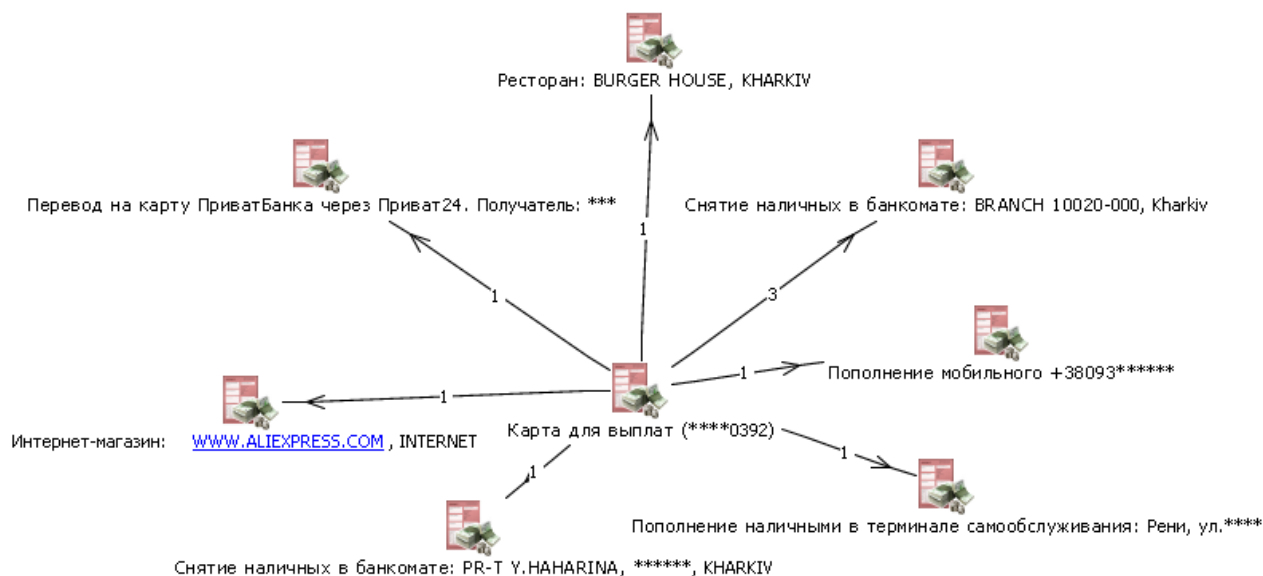
У якості прикладу роботи застосування можна навести аналіз даних про рух коштів на картковому рахунку. Під час імпорту файлу з відповідними відомостями (рис. 6) обираємо необхідні стовпці для аналізу, вид графу тощо.

Строка	1	2	3	4	5	6	7
1	Выписка по ва...						
2	Дата	Время	Категори			Сумма в валют...	Валюта карты
3	01.11.2016	17:20	Прочее			3 475,53	грн
4	30.10.2016	20:22	Выдача наличных	Карта для вып...	Снятие наличн...	- 300,00	грн
5	29.10.2016	20:19	Кафе, бары, ре...	Карта для вып...	Ресторан: BUR...	- 44,00	грн
6	29.10.2016	09:15	Выдача наличных	Карта для вып...	Снятие наличн...	- 50,00	грн
7	27.10.2016	19:44	Пополнение мо...	Карта для вып...	Пополнение мо...	- 51,00	грн
8	25.10.2016	21:56	Переводы	Карта для вып...	Перевод с карт...	497,00	грн
9	23.10.2016	20:01	Выдача наличных	Карта для вып...	Снятие наличн...	- 200,00	грн
10	21.10.2016	19:44	Пополнение мо...	Карта для вып...	Пополнение мо...	- 16,00	грн
11	20.10.2016	12:16	Переводы	Карта для вып...	Перевод на кар...	-1 000,00	грн
12	19.10.2016	21:23	Прочее	Карта для вып...	Пополнение на...	497,50	грн

### Рис. 6. Імпорт даних

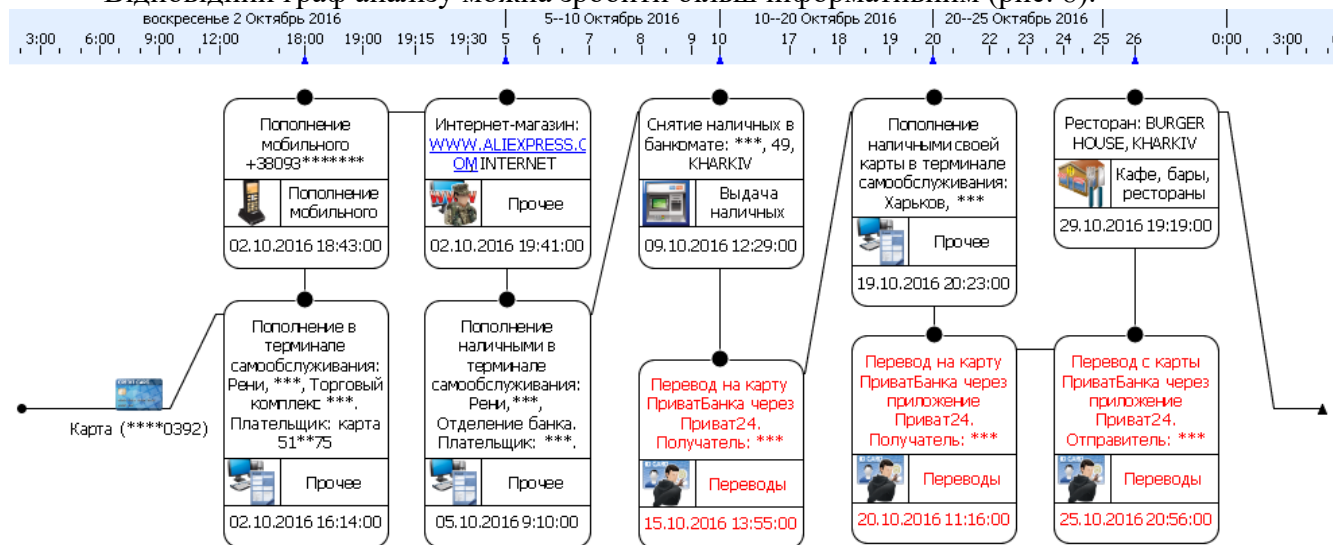


У результаті одержуємо граф для візуального аналізу (рис. 7), з використанням якого можна наочно спостерігати рух коштів по карті.



**Рис. 7. Граф простого аналізу**

Відповідний граф аналізу можна зробити більш інформативним (рис. 8).



**Рис. 8. Більш інформативна часова діаграма**

Для того, щоб збудувати наведену часову діаграму, з використанням інструментів імпорту було видалено зайві символи у полях дати та часу, а потім обрано відповідну ним форму виведення.

1. З використанням програми Maltego CE здійснити аналіз даних з визначеного сайту.
2. З використанням електронних сервісів мобільного зв'язку та онлайн-банкінгу сформувати файли деталізації. Проаналізувати сформовані файли у програмному забезпеченні Maltego CaseFile та IBM i2 Analyst's Notebook. Порівняти одержані результати.

### 3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

#### Рекомендована література

##### Основна

1. Манжай О. В. Курс лекцій з дисципліни.
2. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 p. – URL: [https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal\\_Intelligence\\_for\\_Analysts.pdf](https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf) (дата звернення: 17.05.2023).
3. Ratcliffe J. H. Intelligence-led Policing. 2nd edn. New York, NY: Routledge, 2016. 234 p.
4. Wang Liang & Zhao Jihong Solomon Contemporary police strategies of crime control in U.S. and China: a comparative study. *Crime, Law and Social Change*. 2016. № 5(66). pp. 525-537.
5. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2016. № 3(75). С. 256-265.
6. Потильчак А. О. Щодо співвідношення термінів «кримінальна розвідка» та «кримінальний аналіз» // *Прикарпатський юридичний вісник*. 2017. Вип. 1. Т. 5. С. 174-177.
7. Потильчак А. О. Що таке розвідувальні відомості в контексті моделі Intelligence-Led Policing? // *Visegrad journal on human rights*. 2019. № 6/3. с. 162-166.
8. Манжай О. В., Потильчак А. О. Особливості географічного профілювання у правоохоронних органах // *Право і безпека*. 2020. № 3(78). С. 13-21 (DOI: <https://doi.org/10.32631/pb.2020.3.01>).
9. Манжай О. В., Потильчак А. О. Особливості картографування злочинних проявів // *Право і безпека*. 2020. № 4(79). С. 66-72 (DOI: <https://doi.org/10.32631/pb.2020.4.10>).

##### Допоміжна

10. The National Criminal Intelligence Sharing Plan. Department of Justice. 2003. 54 p. URL: [https://it.ojp.gov/documents/ncisp/National\\_Criminal\\_Intelligence\\_Sharing\\_Plan.pdf](https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf) (дата звернення: 17.05.2023).
11. Манжай О. В., Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic National: Teorie si Practică*. 2015. № 3(13). С. 100-105.

##### Інформаційні ресурси

12. inteltechniques.com