

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

кафедра інформаційних технологій та кібербезпеки, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

до практичних занять

з навчальної дисципліни

Аналітична розвідка у кіберсфері

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

Харків 2020

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО

Вченою радою факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки
(*протокол від 15.09.2020 № 16*)

Розробник:

Доцент кафедри інформаційних технологій та кібербезпеки, к.ю.н., доцент
Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри інформаційних технологій та кібербезпеки
факультету № 4 Харківського національного університету внутрішніх справ к.т.н.,
доцент;

Янович Ю.П., декан факультету права та підприємництва Харківського
університету, к.ю.н., доцент.

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	8
Практичне заняття. Пошук інформації про об'єкти в мережі	9
Практичне заняття. Програмні засоби кримінального аналізу.....	15
3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті	20

1. Розподіл часу навчальної дисципліни за темами

Денна форма навчання

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Вид контролю	
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття		Самостійна робота
Семестр № 2							
Тема № 1 Основні поняття та моделі стримування злочинності	60	10		6	2	42	Екзамен
Тема № 2 Поняття та зміст кримінальної розвідки (зарубіжний досвід)	60	10		8	4	38	
Тема № 3 Розвідка з відкритих джерел (OSINT)	60	10		8	4	38	
Тема № 4 Програмні інструменти кримінальної розвідки	60	10		6	2	42	
Всього за семестр № 2:	240	40		28	12	160	

Заочна форма навчання

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Вид контролю	
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття		Самостійна робота
Семестр № 2							
Тема № 1 Основні поняття та моделі стримування злочинності	58	2		2		54	Екзамен
Тема № 2 Поняття та зміст кримінальної розвідки (зарубіжний досвід)	62	2		2	4	54	
Тема № 3 Розвідка з відкритих джерел (OSINT)	60	2		2	2	54	
Тема № 4 Програмні інструменти кримінальної розвідки	60	4			2	54	
Всього за семестр № 2:	240	10		6	8	216	

Денна форма навчання, іноземці

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 3							
Тема № 1 Основні поняття та моделі стримування злочинності	60	2		2	2	54	Залік
Тема № 2 Поняття та зміст кримінальної розвідки (зарубіжний досвід)	60	4		2	4	50	
Всього за семестр № 2:	120	6		4	6	104	
Семестр № 4							
Тема № 3 Розвідка з відкритих джерел (OSINT)	60	6		4	4	46	Екзамен
Тема № 4 Програмні інструменти кримінальної розвідки	60	4		4	6	46	
Всього за семестр № 4:	120	10		8	10	92	

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 *¹ 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.

¹ Час проведення заняття визначається згідно з програмою

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 обом 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. Ratcliffe J. H., Guidetti R. State police investigative structure and the adoption of intelligence-led policing. *Policing: An International Journal of Police Strategies & Management*. 2008. Vol. 31. Iss. 1. pp. 109-128 (DOI 10.1108/13639510810852602).
2. 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.
3. 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)
4. Ratcliffe J. The Effectiveness of Police Intelligence Management: A New Zealand Case Study. *Police Practice and Research: An International Journal*. – 2005. Vol. 6. No. 5. pp. 435-451.
5. 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.
6. Maguire M. & John T. Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK. *Policing and Society: An International Journal of Research and Policy*. 2006. Vol. 16. No. 1. pp. 67-85 (DOI: 10.1080/10439460500399791).
7. Dai Mengyan Policing in the People's Republic of China: a review of recent literature. *Crime, Law and Social Change*. 2008. № 50(3). pp. 211-227 (DOI 10.1007/s10611-008-9131-7).
8. Chen Xiaoming Community and Policing Strategies: A Chinese Approach to Crime Control. *Policing and Society: An International Journal of Research and Policy*. 2002. Vol. 12. No. 1. pp. 1-13. DOI: 10.1080/10439460290006646.
9. Ma Yue The powers of the police and the rights of suspects under the amended Criminal Procedure Law of China. *Policing: An International Journal of Police Strategies & Management*, 2003. Vol. 26. Iss 3. pp. 490-510.
10. Tilley N. Problem-Oriented Policing, Intelligence-Led Policing and the National Intelligence Model. London: Jill Dando Institute of Crime Science, 2003. URL: <https://pdfs.semanticscholar.org/bb06/7c510c954889cd85be02890e6cb698e70ddf.pdf> (Дата звернення: 11.12.2107).
11. Innes M., Sheptycki J. W. E. From Detection to Disruption: Intelligence and the Changing Logic of Police Crime Control in the United Kingdom. *International Criminal Justice Review*. 2004. Vol. 14. pp. 1-24.

12. Водько Н. П. О содержании термина «криминальная разведка». *Південноукраїнський правничий часопис*. 2016. № 1. С. 83-85.
13. 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).
14. 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.
15. Албул С. В., Користін О. Є. Концепція розвитку кримінальної розвідки органів внутрішніх справ України. *Південноукраїнський правничий часопис*. 2015. № 1. С. 158-163.
16. Brown S. D. The meaning of criminal intelligence. *International Journal of Police Science & Management*. 2007. Vol. 9. No 4. pp. 336-340.
17. 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.
18. 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.
19. 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 *¹ год. Місце проведення: навчальна аудиторія.
(кількість годин) (полігон, комп'ютерний клас, лабораторія, лінгафонний кабінет)

Вхідні дані (взято з навчальної практики для британських поліцейських):

1. Оперативне зведення 67/12 - Інформатор 1445 ідентифікував МОПРОУ як фахівця зі схем планованого банкрутства і махінацій з пенсійними фондами, і як можливого співника ЛОУРІ. [В-2].

2. Зведення з моніторингу фінансової діяльності 594/12 – УАЙЛІ ідентифікований як президент, а ЛОУРІ – як бухгалтер компанії «Rexford Investments Inc». [А-1].

3. Оперативне зведення 84/12 – під час спостереження ЛОУРІ був помічений на зустрічі приблизно 15 чоловік в ресторані «Боброва голова» (Beaver Head Restaurant). Для групи був відкритий бар і буфет у відгородженій секції в кімнаті відпочинку. ЛОУРІ стверджує, що він є фінансовим генієм у сфері злиття і поглинання бізнесу, а також в управлінні власністю. Один з людей в групі був ідентифікований як СМІТ. [А-1].

4. Оперативне зведення 89/12 – СМІТ і РОУ були заарештовані разом за неправомірне проникнення з метою вчинення злочинних дій до місцевого офісу компанії-франчайзі «Happiness Travel Service» (Склад номер 14). Надалі власники офісу компанії відмовилися від звинувачень. РОУ є віце-президентом «Happiness Travel Services Inc». [А-1].

5. Зведення з моніторингу фінансової діяльності 603/12 – щодо ДЕЙНА і його компанії «DANE Pension Planning Services» проводиться розслідування Міністерством Праці за порушення положень Закону про захист пенсійного доходу. [А-1].

6. Оперативне зведення 117/12 – Компанія «Rexford Investments Inc» є клієнтом компанії «DANE Pension Planning Services». [А-1].

7. Зведення з моніторингу фінансової діяльності 676/12 – УАЙЛІ є основним акціонером та президентом компанії «Commercial Realty Inc.» Компанія «Commercial Realty Inc.» була залучена до низки великих операцій з продажу та обміну комерційної нерухомості протягом останніх шести місяців. [А-1].

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.

Література, методичне та матеріально-технічне забезпечення занять

1. Criminal Intelligence. Manual for Analysts [Електронний ресурс]. – United Nations, 2011. – 96 с.
2. Guidance on the National Intelligence Model [Електронний ресурс] / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. – 2005. – 213 с. – Режим доступу: <https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf>.

¹ Час проведення заняття визначається згідно з програмою

3. The National Criminal Intelligence Sharing Plan [Електронний ресурс] / Department of Justice. – 2003. – 54 с. – Режим доступу: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf.

4. 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.

5. 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.

6. National Intelligence Model: Code of Practice [Електронний ресурс]. – CENTREX, 2005. – 14 с. – Режим доступу: <http://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf>.

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 *¹ 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 злочином, 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;

- набір інструментів для збирання інформації з відкритих джерел osintframework.com, inteltechniques.com;

- агрегатор інформації про юридичних осіб youcontrol.com.ua, iplex.com.ua/;

- пошук у базах даних кадрових агентств (наприклад, work.ua /реєстрація як підприємець/);

- пошук у сервісах телефонних номерів (www.truecaller.com, sync.me, findnumberapp.com);

- сервіс пошуку розташування точок доступу Wi-Fi за MAC-адресою або назвою (для пошуку потрібно зареєструватись) wigle.net;

- боти (наприклад, для Telegram: @OpenDataUABot, @e007bot, @OpenDeclarationBot, @d_TarasBotagent);

¹ Час проведення заняття визначається згідно з програмою

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

Окрім наведеного велику *бібліотеку пошукових ресурсів* можна завантажити за посиланням <http://osint.academy/2016/10/20/biblioteka-otkrytyh-istochnikov/>.

Вхідні дані.

Таблиця 1. Оператори Яндекс

Оператори	Значення	Приклад
«»	Слова розташовані підряд у точній формі.	«торгівля людьми»
«слово*слово»	Пропущено слово у виразі	«надання * послуг»
& (логічне І)	Слова в межах одного речення.	дитяче&порно
&&	Слова у межах одного документа	робота && інтим
(логічне АБО)	Пошук будь-якого зі слів	порно «продаж органів»
()	Дужки формують групи у складних запитах	(Інтим Україна) & (Київ Буча)
-	Вилучення слова з пошуку	органи ~ Київ
/ 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 + Туреччина
!	Слово в точній формі з заданим регістром	! фірма «Чайка»
!!	Словникова форма слова	!!віза
title:	Пошук за заголовками документів	title:Органи з України
url:	Пошук за URL	url:www.ttt.tt/log/
inurl:	Пошук за фрагментом URL	inurl:xxx
host:	Пошук за хостом	host:www.yandex.ru
rhost:	Пошук за хостом у зворотному записі	rhost:com.livejournal.*
mime:	Пошук за одним типом файлів	mime:jpg
lang:	Пошук з обмеженням за мовою	lang:ua
domain:	Пошук з обмеженням за доменом	domain:ua
date:	Пошук з обмеженням за датою	date:201501*
date:дата, date:> дата	Пошук з обмеженням за інтервалом дат	date:20141215..20150101, date:>20141231
cat:	Пошук за рубрикою Яндекс.Каталогу	cat:11000051

Таблиця 2. 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

Оператори	Значення	Приклад
—	Зв'язування двох слів.	швидкий заробіток
..	Пошук цифр у заданому діапазоні	\$50..\$100
@	Пошук електронної пошти	@google
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:опрани
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 3. 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		
		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		
2.	Географічні дані / Місце розташування (питання «Де?» та «Як знайти?»)	Паролі		
		Місце народження		
		Домашня адреса (місце реєстрації, місце фактичного проживання)		
		Телефонний номер (проводова лінія)		
		Поштова адреса		
		Кабельне телебачення		
		Мобільний телефон		
		Транспортний засіб та інше рухоме		

№ з/п	Критерій	Ознака	Значення	Джерело
		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.	Часові характеристики (питання «Коли?»)	Дата і час певної події		
4.	Зв'язки (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.	Сфера інтересів (питання «Чим цікавиться?»)	Транспортні засоби		
		Зброя		
		Тварини		
		Техніка		
		Мистецтво		
		Колекціонування		
		Контрабанда		
		Землі, будівлі, бізнес-структури		
6.	Фактичні обставини (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.	Системна характеристика (питання «Яка особа?»)	Громадянська позиція		
		Професійні якості		
		Державна служба		
		Відгуки колективу		
		Результати тестувань (медичного,		

№ з/п	Критерій	Ознака	Значення	Джерело
		професійного, психологічного)		
		Самохарактеристика		
		Показники кредитоспроможності		
		Страхові рейтинги		

Корисні ресурси

Мережні сховища	– https://cloud.mail.ru , https://www.dropbox.com , https://yadi.sk , https://drive.google.com , https://mega.co.nz , http://www.ge.tt
Перелік існуючих безкоштовних VPN-мереж	– http://www.makeuseof.com/tag/7-completely-free-vpn-services-protect-privacy
Пошук видалених сторінок	– http://www.cachedpages.com/ http://www.archive.org/
Пошук завантажень з визначеної IP-адреси	– https://iknowwhatyoudownload.com/ru/peer/
Пошук за різними установчими даними	– http://www.nomer.org , http://www.yasni.ru , http://www.radaris.com http://lookup.com https://www.imena.ua/blog/ukraine-database/ http://osintframework.com/ https://youcontrol.com.ua http://findmobil.info/
Пошук зображення особи	– http://www.facesaerch.com , http://www.tofinder.ru/index.php , https://images.google.com/imghp?tbm=isch&tbs=itp:fface&gws_rd=ssl , http://images.yandex.ru/yandsearch?type=face
Пошук за зображенням	– http://www.findbyface.com/ https://findface.ru/
Пошук зображень (копій)	– http://images.google.com , http://images.yandex.ua , http://images.search.yahoo.com , http://www.tineye.com ,
Пошук контактів «Первоискатель»	– http://pervoiskatel.ru
Пошук людей за прізвищем в соціальних мережах	– http://socpoisk.com , http://www.ph4.ru/service_socsearch.ph4?a=social
Пошук по онлайн щоденниках	– http://www.liveinternet.ru , http://www.livejournal.com , http://tumblr.com
Пошук по профілях Google+	– http://google.com/profiles
Пошук по сервісах обміну фотографіями і відеозаписами	– http://www.youtube.com , http://rutube.ru , http://instagram.com ,

Пошук серед осіб, які поступали у вищі навчальні заклади України	–	http://flickr.com , http://picasa.google.com http://vstup.info
Сервіси для збирання інформації про електронні ресурси за адресами	–	http://robtex.com , http://he.net
Соціальні мережі	–	http://vk.com , http://odnoklasniki.ru , http://facebook.com , http://my.mail.ru , http://plus.google.com , http://myspace.com , http://mirtesen.ru , http://moikrug.ru http://vkrugudruzei.ru , http://gidepark.ru
Яндекс.Пошук людей в соціальних мережах (Вконтакте, Facebook, Twitter, GooglePlus, МойКруг, Livejournal, Яру)	–	http://people.yandex.ru
WEB-архіви	–	http://archive.is/ , http://archive.org/
Пошук розташування точок доступу Wi-Fi за MAC-адресою або назвою (для пошуку потрібно зареєструватись)	–	https://www.wigle.net/
Фішингові сайти	–	https://ema.com.ua/report-an-incident/black-list/
Форум із обговореннями різних протиправних технік (у тому числі зламані бази)	–	http://phreaker.pro/

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. Каліжєвський, 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 *¹ 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**
 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) 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).

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 випадяючому списку в меню Run View. На рис. 1 наведено приклад аналізу за базовим методом Footprint L1 сайту 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.

¹ Час проведення заняття визначається згідно з програмою

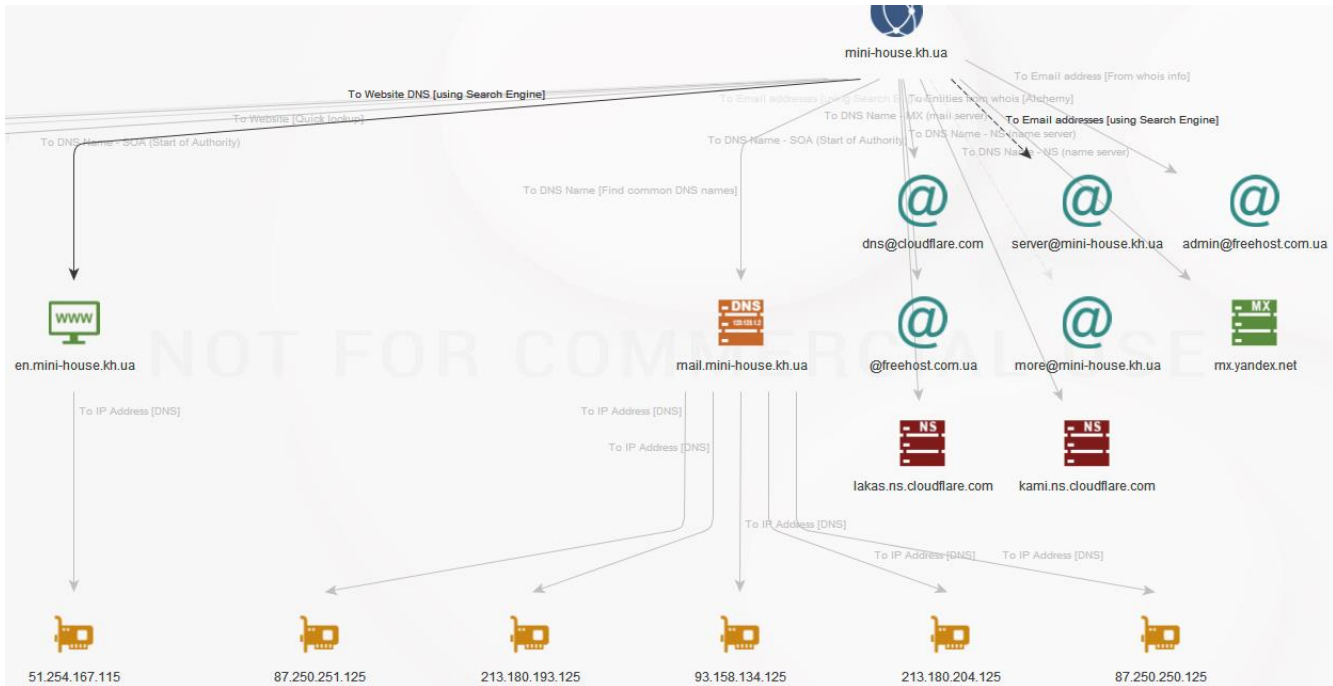


Рис. 1. Результат аналізу сайту

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).

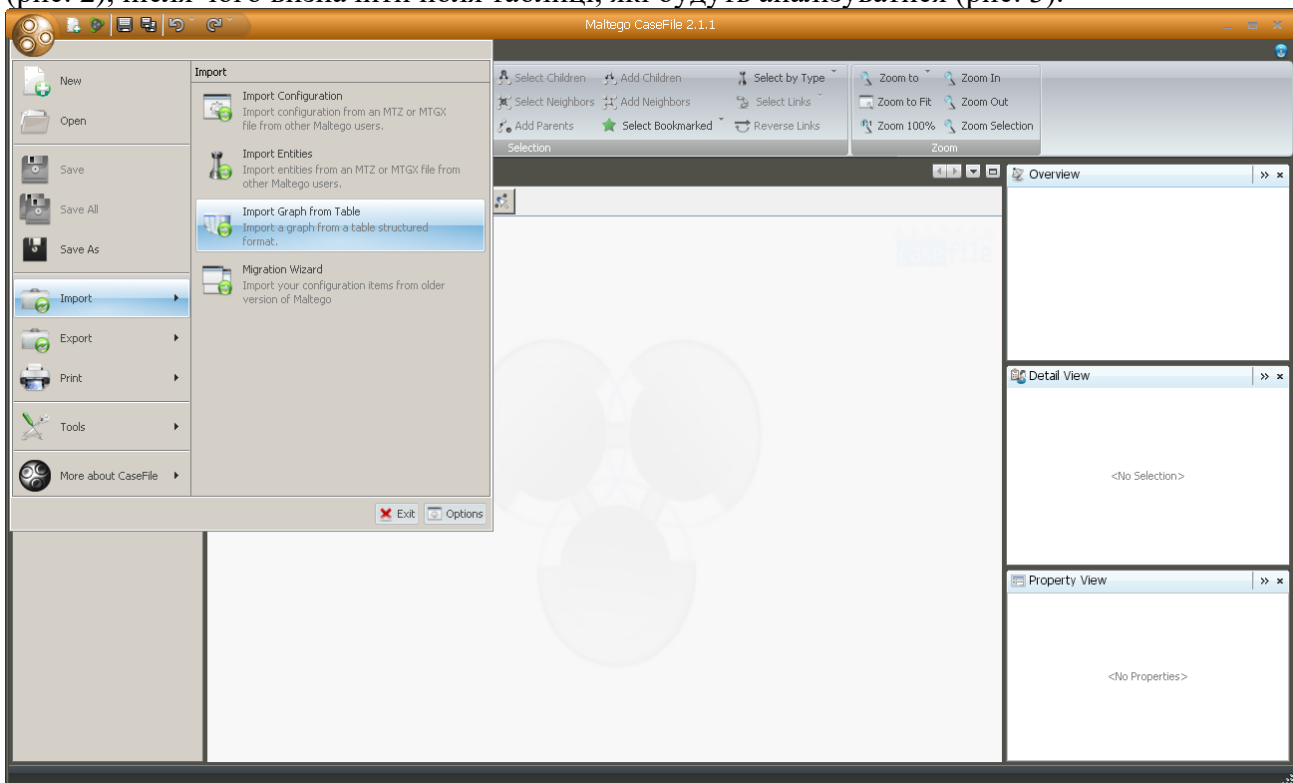


Рис. 2. Імпорт локальних даних до програми Maltego CaseFile

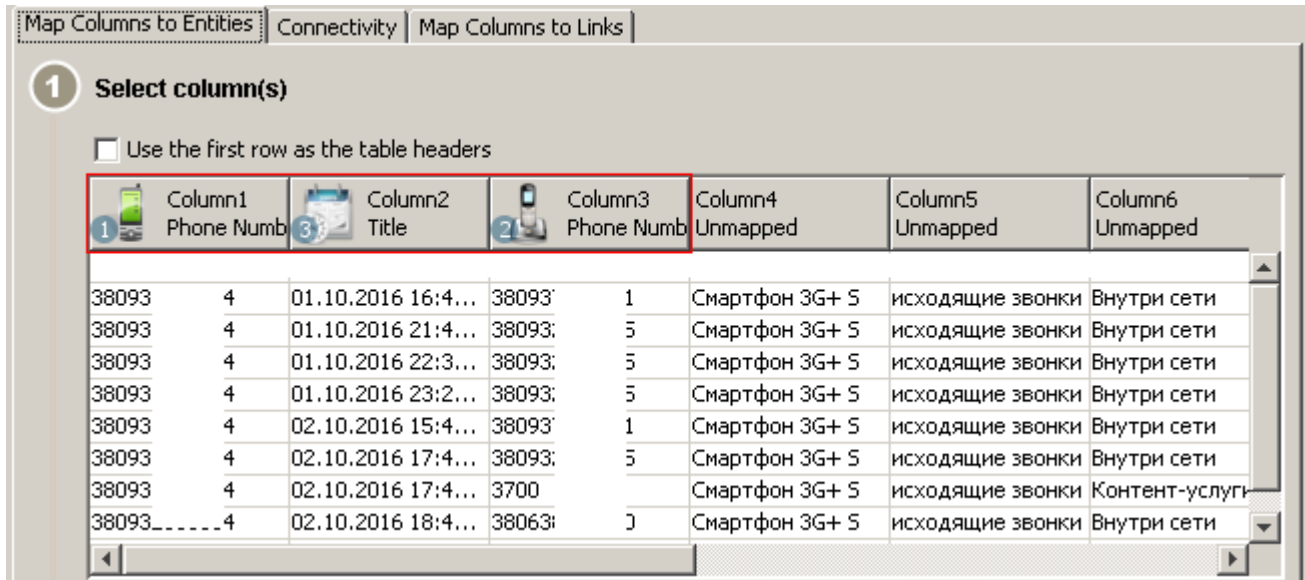


Рис. 3. Визначення даних для аналізу

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

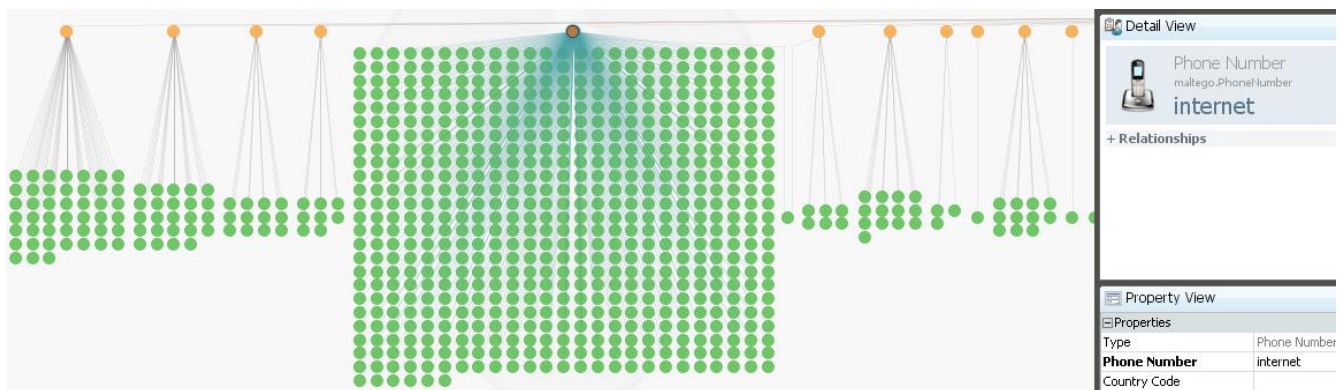


Рис. 4. Результати аналізу

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.

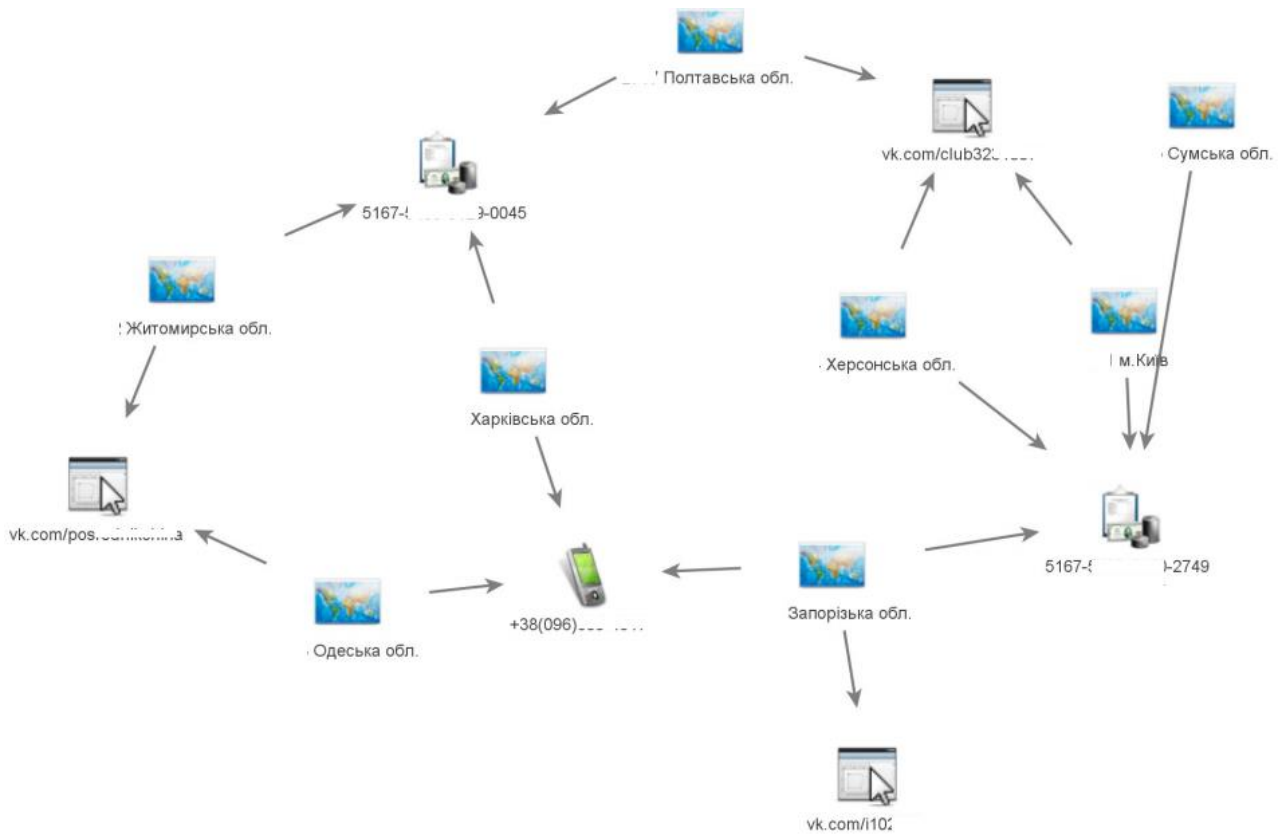


Рис. 5. Фрагмент діаграми

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.

Включить выделенную строку (строки) Исключить выделенную строку (строки) Задать строку заголовка							
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.

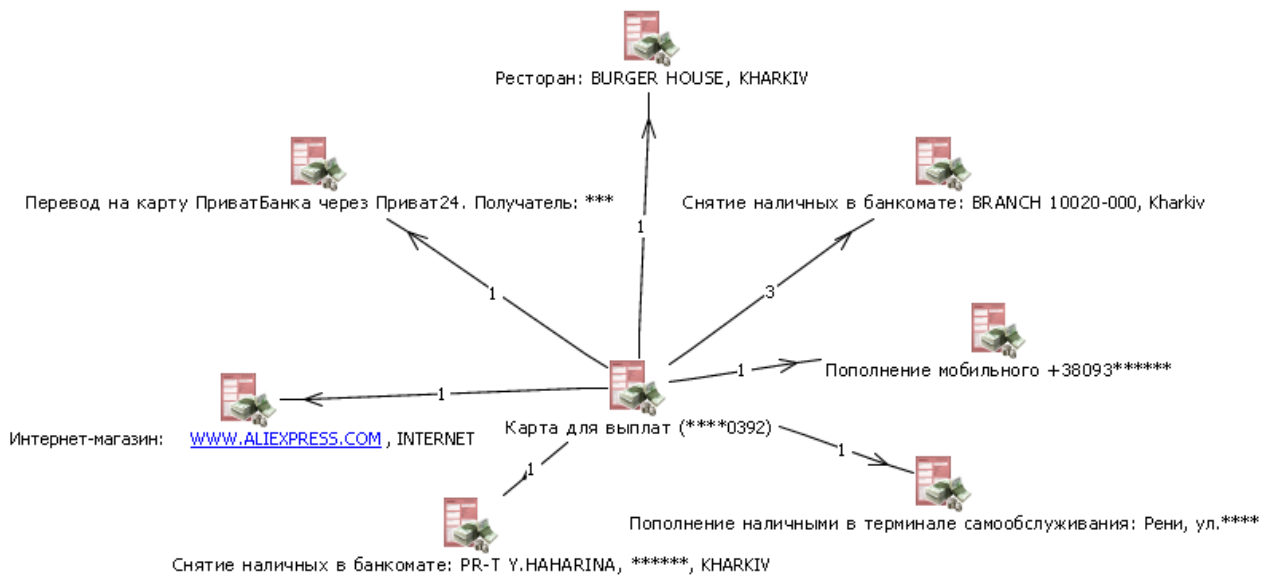


Рис. 7. Граф простого аналізу

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

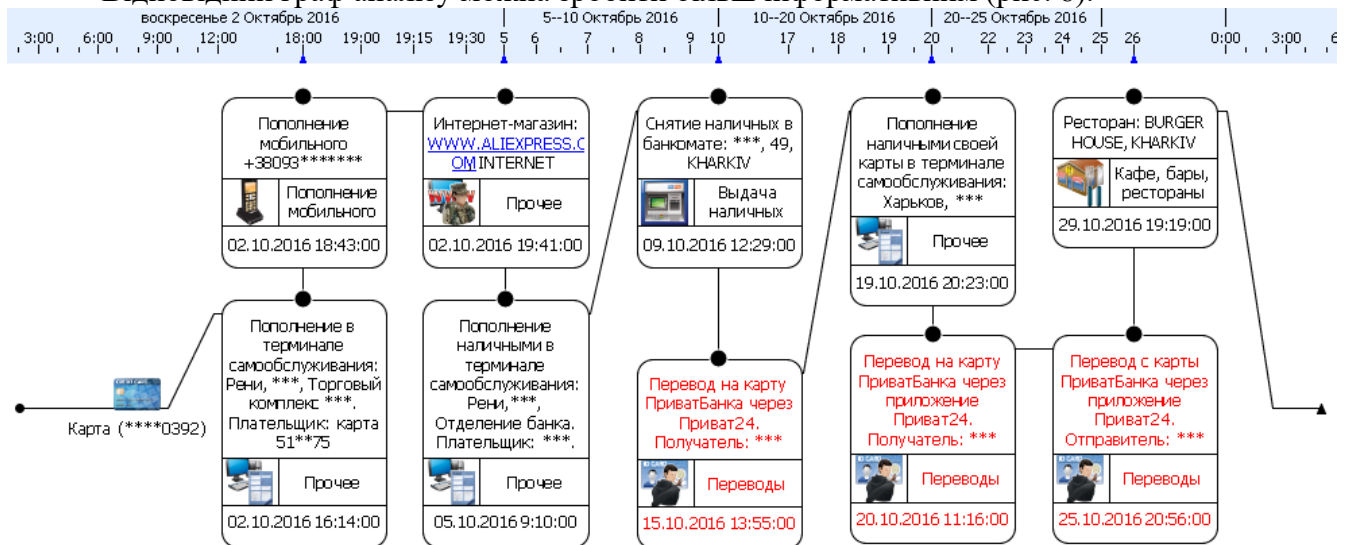


Рис. 8. Більш інформативна часова діаграма

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 «Аналітична розвідка у кіберсфері».
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 (дата звернення: 17.10.2017).
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.

Допоміжна

6. Brown S. D. The meaning of criminal intelligence. *International Journal of Police Science & Management*. 2007. Vol. 9. No 4. pp. 336-340.
7. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. 2005. 213 с. URL: <https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf> (дата звернення: 17.10.2020).
8. National Intelligence Model: Code of Practice. CENTREX, 2005. 14 p. URL: <http://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf> (дата звернення: 17.10.2020).
9. Ratcliffe J. H., Guidetti R. State police investigative structure and the adoption of intelligence-led policing. *Policing: An International Journal of Police Strategies & Management*. 2008. Vol. 31. Iss 1. P. 109-128 (DOI 10.1108/13639510810852602).
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 (дата звернення: 17.10.2020).
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. Персональний комп'ютер зі встановленою операційною системою Windows 7 або вище та доступом до локальної та глобальної мережі.
13. inteltechniques.com.