

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

кафедра інформаційних технологій та кібербезпеки, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

до лабораторних 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.

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 № 2 Поняття та зміст кримінальної розвідки (зарубіжний досвід)

Лабораторне заняття. Порівняльний аналіз справ. Складання аналітичних висновків.

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)

Завдання 1

Провести порівняльний аналіз описаних подій, результати слід представити у табличному вигляді. На підставі аналізу результатів порівняння підготувати аналітичний висновок.

Вхідні дані:

Орієнтування 1

Увечері п'ятниці 20 грудня 17-річний студент Девід Ф. та 16-річна студентка Бетті Д. пішли на побачення. Пара планувала відвідати різдвяний концерт неподалік від дому Бетті. Натомість на автомобілі «Ремблер», що належав матері Девіда вони поїхали в гості до приятельки, після чого вечеряли у місцевому ресторані. По завершенні вечери пара поїхала на автомобілі вздовж місцевого озера та близько 22:15 припаркувала автомобіль на стоянці, знаній як «місце для побачень». Невдовзі за автомобілем студентів зупинився інший автомобіль, з якого вийшла людина та звеліла студентам виходити з машини. Спочатку вийшла студентка, а потім Девід. Особа, яка звеліла вийти студентам, зробила постріл у Девіда. Бетті, намагаючись втекти, відбігла

¹ Час проведення заняття визначається згідно з програмою

на 8,5 м. За цей час вбивця вистрілив у неї п'ять разів та поїхав. Після 23:00 трупи обох жертв виявили місцеві мешканці.

Орієнтування 2

У п'ятницю 4 липня наступного року після нападу на студентів Девіда Ф. та Бетті Д. сталася інша подія. Близько 00:00 Дарлін Ф. та Майкл М. на автомобілі Шевроле припарковалися біля парку, що розташовувався на відстані 6,4 км від місця нападу на Девіда Ф. та Бетті Д. За 10 хвилин позаду Шевроле припарковався інший автомобіль, який спочатку поїхав, проте за 5-10 хвилин знову повернувся. З цього автомобіля вийшов чоловік з ліхтарем та підійшов до Шевроле з боку пасажирського сидіння, де знаходився Майкл М. Чоловік, підсвічуючи ліхтарем, зробив п'ять прицільних пострілів по пасажирів Шевроле з пістолету «Люгер» калібру 9 мм. Залишаючи місце події, злочинець почув стогін Майкла М., повернувся та виконав ще по два постріли в кожну жертву. Після цього чоловік поїхав з місця події. У результаті отриманих травм Дарлін Ф. загинула. Майклу М. вдалося вижити.

Наступного дня о 00:40 злочинець зателефонував в поліцію та повідомив про вчинення злочину, а також взяв на себе відповідальність за вбивство «тих хлоп'ят минулого року».

Орієнтування 3

У суботу 27 вересня того ж року, коли стався напад на Дарлін Ф. та Майкла М., відбулася ще одна подія. Брайан Х. та Сесілія Енн Ш. відпочивали біля озера на острові, поєднаному із сушею пісочною косою, коли о 18:20 до них підійшов чоловік, одягнений у фартух з емблемою у вигляді перекресленого кола та чорний капюшон ката. При цьому отвори для очей було прикрито сонцезахисними окулярами. При собі чоловік мав пістолет та ніж. Він пояснив, що є злочинцем, який втік з-під варті і йому потрібні гроші та автомобіль, щоб виїхати до Мексики. Чоловік дав Сесілії Енн Ш. мотузку, якою наказав зв'язати Брайана Х. Після цього зловмисник зв'язав Сесілію Енн Ш. Брайан Х. вступив в діалог з нападником, останній продемонстрував йому споряджений магазин, проте заявив, що застосує проти них ніж. Після цього зловмисник ножем наніс серію ударів обом жертвам. Після цього нападник намалював на автомобілі Брайана Х. закреслене коло. Згодом злочинець зателефонував до поліції та повідомив про злочин. Сесілії Енн Ш. було нанесено 24 удари ножем, проте коли її виявили вона була притомна та змогла докладно описати злочинця. Згодом вона померла, Брайан Х. вижив. На місці вчинення злочину виявили слід армійського черевика.

Орієнтування 4

У суботу 11 жовтня того ж року, коли трапилася попередня подія, близько 21:40 до автомобіля таксиста Пола С. сів пасажир та попросив підвезти його до перехрестя вулиць В. та М. О 21:55 таксі зупинилося за квартал від обумовленого місця висадки на розі вулиць В. та Ч. Пасажир вбив Пола С. пострілом у голову з пістолету калібру 9 мм. Вбивця забрав із собою ключі від автомобіля, гаманець та частину сорочки жертви. Це побачили свідки, які викликали поліцію, а також повідомили, що вбивця витер сліди свого перебування у таксі. Пізніше вбивця зателефонував у поліцію та повідомив, що його зупиняли патрульні, проте не запідозрили у ньому злочинця.

Орієнтування 5

У неділю 22 березня наступного року після вбивства Пола С. 23-річна вагітна Кетлін Д. із 10-місячною донькою їхала до своєї матері в інше місто. Дорогою їй почав сигналізувати водій, який вказав на погане кріплення правого заднього колеса та запропонував допомогти з його фіксацією, на що жінка погодилась. За деякий час після «ремонт» колеса відвалилося, а «ремонтник-водій» запропонував підвезти Кетлін Д. з донькою до найближчої автозаправної станції. Незнайомець возив пасажирок декілька годин, а на запитання Кетлін Д., чому він не зупиняється біля заправок, переводив тему розмови. За деякий час водій зупинився на перехресті та повідомив жінку, що вб'є її, а доньку викине. Почувши це, жінка схопила доньку, виплигнула з автомобіля та сховалася у полі. Пізніше вона попутним автомобілем доїхала до поліції, де повідомила про те, що сталося. В поліції Кетлін Д. звернула увагу на портрет підозрюваного у

вбивстві Пола С. та вказала, що саме цей чоловік погрожував їй. За деякий час автомобіль Кетлін С. знайшли зпаленим. Як вважається, це зробила та сама особа, з якою контактувала жертва.

Завдання 2

Скласти аналітичний висновок

Вхідні дані: на місці події було вилучено ноутбук особи, яка ймовірно причетна до вчинення злочину. За результатами проведення огляду ноутбуку висунуто одну з версій, що даний пристрій ймовірно використовувався лише для доступу в мережу Інтернет, при цьому застосовувався Тог-браузер. Операційна система неліцензійна Windows 8.1. У протоколі огляду пристрою було також зазначено, що у пам'яті комп'ютера збереглися назви точок доступу для підключення WiFi (PodVodouy, Sladkiy Pinguin, Gomechko_Room344). Також у наявності є фоторобот підозрюваного – власника ноутбуку.

Порядок проведення заняття

1. Групу розділяють на три команди.
2. Кожній команді потрібно провести порівняльний аналіз справ та підготувати аналітичний висновок. Дозволяється користуватися сервісом (wagle.net).
3. Підбиваються підсумки.

Література, методичне та матеріально-технічне забезпечення занять

1. Criminal Intelligence. Manual for Analysts. 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>.
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)

Лабораторна робота. Інформаційні технології для пошуку та аналізу даних з соціальних мереж

Навчальна мета заняття: отримати практичні навички пошуку та аналізу даних з соціальних мереж за допомогою відкритих мережних ресурсів.

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 2000 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**

Суттєву користь для аналізу профілів соціальних мереж можуть надати онлайн-ресурси. З метою встановлення відомостей про торговців людьми, які застосовують соціальні мережі, можна використовувати відповідні онлайн-сервіси.

Наприклад, для соціальної мережі «Вконтакте» існують сервіси для аналізу:

- віртуалізація контактів, вказаних у профілі (yasiv.com/vk/);
- сервіс для визначення переліку профілів, яким досліджувана особа ставить «лайки» (застосунок «Кого лайкає мой друг? Найдем все лайки :»);
- агрегатор різних даних (vk.city4me.com);

Для пошуку в соціальній мережі Вконтакте фотознімків, зроблених на певній території, вельми корисною є утиліта photobygeo.py (<https://bitbucket.org/BetepokNoname/photobygeo/overview>). Відпочатку дана програма дозволяла здійснювати аналогічний пошук в Instagram, однак надання відповідної API-функції для використання сторонніми застосунками було припинено власником цієї соціальної мережі.

Для того, щоб скористатися можливостями скрипта photobygeo.py у Windows, слід встановити python (<https://www.python.org/downloads/release/python-2714/>), бібліотеку requests (<https://pypi.python.org/pypi/requests/2.18.4#downloads>). Встановлення бібліотеки досягається вилученням з архіву відповідних файлів бібліотеки та наступним запуском `python setup.py install` з командного рядка у папці з вилученою бібліотекою.

Для роботи зі скриптом достатньо ввести чотири параметри: широту, довготу, початковий та кінцевий час для пошуку.

Наприклад,

```
python photobygeo.py 49.935441 36.276979 1460408400 1460667600
```

У даному випадку здійснюватиметься пошук фотознімків, геокоординати яких містяться в радіусі 100 метрів навколо 5-го корпусу ХНУВС у період з 00:00:00 12.04.2016 до 00:00:00 15.04.2016.

Радіус пошуку та деякі інші параметри задаються безпосередньо у вихідному коді скрипта.

Результати зберігаються у файлі HTML в папці користувача або папці з програмою Python, наприклад, C:\Users\Pcname або C:\Python.

Дізнатися координати на мапі можна з використанням відповідного сервісу Google Maps (<https://www.google.ru/maps>).

Приклади сервісів для переведення звичного часу у timestamp знаходяться за адресами <http://www.timestampgenerator.com/> або <http://www.bl2.ru/programing/timestamp.html>.

Також існує сервіс, який автоматизує зазначені процедури через веб-форму: <http://snradar.azurewebsites.net/>.

Зареєструвати у відповідній соціальній мережі профіль (друзів не додавати).

З використанням описаних ресурсів здійснити аналіз одного з профілів в соціальній мережі.

Результат у формі тез-висновків відобразити у текстовому файлі.

¹ Час проведення заняття визначається згідно з програмою

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**Лабораторне заняття. Географічне профілювання**

Навчальна мета заняття: отримати практичні навички складання географічних профілів.

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 7 або вище та доступом до мережі Інтернет, Excel 2013 або вище.

З використанням пакету 3D Maps MS Excel скласти динамічну теплову мапу злочинності навколо аеропорту (радіус 500 м). Після цього скласти географічний профіль правопорушника за завданням викладача.

Результати відобразити у звіті.

¹ Час проведення заняття визначається згідно з програмою

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: 17.10.2020).
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: 17.10.2017).
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.