

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра інформаційних технологій та кібербезпеки, факультет № 4

ПРОГРАМА

навчальної дисципліни «Кримінальна 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.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Програма *вибіркової* навчальної дисципліни складена відповідно до освітньої програми *другого* рівня вищої освіти *спеціальності «Кібербезпека» спеціалізації «Протидія кіберзлочинності»*.

Предметом вивчення навчальної дисципліни є особливості використання аналітичного апарату для накопичення та обробки даних з кіберпростору

Міждисциплінарні зв'язки: «Моделі, методи та засоби аналітичної обробки великих масивів даних», «Методика наукових досліджень».

Програма навчальної дисципліни складається з таких тем:

1. Основні поняття та моделі стримування злочинності.
2. Поняття та зміст кримінальної розвідки (зарубіжний досвід).
3. Розвідка з відкритих джерел (OSINT).
4. Програмні інструменти кримінальної розвідки.

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни «Аналітична розвідка у кіберсфері» є засвоєння особливостей використання комп'ютерних технологій з метою накопичення, обробки та аналізу інформації.

1.2. Завданнями вивчення дисципліни «Аналітична розвідка у кіберсфері» є аналіз різних моделей стримування злочинності; дослідження поняття, завдання та функції кримінальної розвідки у кіберсфері; аналіз зарубіжного досвіду кримінальної розвідки у кіберсфері; вивчення особливостей здійснення розвідки з відкритих джерел; одержання навичок роботи з інструментами кримінальної розвідки.

1.3. Згідно з освітньою програмою здобувачі вищої освіти повинні:

знати:

- особливості здійснення кримінальної розвідки у кіберсфері;
- особливості застосування різних програм для пошуку інформації у кіберсфері;
- моделі стримування злочинності;
- зарубіжний досвід здійснення кримінальної розвідки;

вміти:

- застосовувати норми законодавства для здійснення аналітичної роботи;
- складати аналітичні висновки та представляти їх замовнику;
- застосовувати програмні засоби аналізу із графічним відображенням отриманих результатів;
- здійснювати віддалений збір інформації про вузли комп'ютерної мережі;
- шукати інформацію про об'єкти в мережі;

бути ознайомленими:

- з особливостями функціонування систем накопичення та обробки інформації.

1.4. Форма підсумкового контролю (екзамен)

На вивчення навчальної дисципліни відводиться 240 годин / 8 кредитів ECTS.

1.5. Програмні компетентності:

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність		Здатність самостійно досліджувати і розроблювати комплексні системи забезпечення кібербезпеки, викладати і здійснювати аналітичну діяльність в області кібербезпеки
Загальні компетентності (ЗК)	ЗК.2	Здатність приймати управлінські й обґрунтовані рішення в складних і непередбачуваних умовах
Спеціальні (фахові, предметні) компетентності (ФК)	ФК.3	Здатність будувати відповідні моделі сценаріїв кіберризиків, досліджувати їх для отримання нових висновків та поглиблення розуміння природи кіберзагроз

2. Короткий опис змісту навчальної дисципліни

Тема № 1. Основні поняття та моделі стримування злочинності.

Залучення суспільства до вирішення завдань правоохоронної діяльності (community policing). Модель нульової толерантності (zero tolerance policing). Проблемно-орієнтована модель (problem-oriented policing). Модель небезпечних зон (hot spots policing). Модель на основі розвідувальних даних (intelligence-led policing). Прогностична модель (predictive policing).

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

Сенс кримінальної розвідки. Стратегії кримінальної розвідки. Види кримінальної розвідки (стратегічна, тактична, оперативна). Засоби кримінальної розвідки. Етапи кримінальної розвідки.

Тема № 3. Розвідка з відкритих джерел (OSINT).

Джерела відкритої інформації. Пошук інформації про об'єкти в мережі. Аналіз профілів соціальних мереж. Систематизація одержаної інформації.

Тема № 4. Програмні інструменти кримінальної розвідки.

Загальні інструменти для аналізу даних. Інструменти картографічного профілювання.

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

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 (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: 17.10.2020).
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. inteltechniques.com

4. Засоби оцінювання здобувачів вищої освіти

1. Залучення суспільства до вирішення завдань правоохоронної діяльності (community policing).
2. Моделі стримування злочинності.
3. Модель нульової толерантності (zero tolerance policing).
4. Проблемно-орієнтована модель (problem-oriented policing).
5. Модель небезпечних зон (hot spots policing).
6. Модель на основі розвідувальних даних (intelligence-led policing).
7. Прогностична модель (predictive policing).

8. Сенс кримінальної розвідки.
9. Стратегії кримінальної розвідки.
10. Види кримінальної розвідки.
11. Стратегічна кримінальна розвідка.
12. Інструменти і методи стратегічної кримінальної розвідки.
13. Тактична кримінальна розвідка.
14. Інструменти і методи тактичної кримінальної розвідки.
15. Оперативна кримінальна розвідка.
16. Інструменти і методи оперативної кримінальної розвідки.
17. Засоби кримінальної розвідки.
18. Застосування методології Анасара у кримінальній розвідці.
19. Етапи кримінальної розвідки.
20. Постановка завдань як етап здійснення кримінальної розвідки.
21. Збирання даних як етап здійснення кримінальної розвідки.
22. Оцінка даних як етап здійснення кримінальної розвідки.
23. Системи оцінки 4x4, 5x5, 6x6.
24. Обробка даних як етап здійснення кримінальної розвідки.
25. Аналіз даних як етап здійснення кримінальної розвідки.
26. Дерево зв'язків (link charting).
27. Дерево подій (event charting).
28. Дерево цінностей (commodity flow charting).
29. Дерево дій (activity charting).
30. Фінансове профілювання (financial profiling).
31. Частотний графік (frequency charting).
32. Кореляція даних (data correlation)
33. Мережний аналіз даних.
34. Особливості побудови діаграм за даними про телефонні з'єднання.
35. Розробка аналітичних висновків як етап здійснення кримінальної розвідки.
36. Види аналітичних висновків.
37. Зміст аналітичних висновків. Система запитань 5W+H.
38. Етапи проведення аналізу конкуруючих гіпотез.
39. Поширення інформації як етап здійснення кримінальної розвідки.
40. Повторний аналіз інформації.
41. Джерела відкритої інформації.
42. Пошук інформації про об'єкти в мережі.
43. Збирання інформації про мережі даних.
44. Аналіз профілів соціальних мереж.
45. Методи встановлення IP-адреси.
46. Аналіз заголовків електронних документів.
47. Аналіз метаданих.
48. Систематизація одержаної інформації.
49. Загальні інструменти для аналізу даних.
50. Сенс та завдання картографування злочинних проявів.

- 51.Інструменти картографічного профілювання.
- 52.Використання MS Excel для вирішення завдань кримінальної розвідки.
- 53.Використання IBM i2 для вирішення завдань кримінальної розвідки.
- 54.Використання Palantir для вирішення завдань кримінальної розвідки.
- 55.Використання Maltego для вирішення завдань кримінальної розвідки.
- 56.Використання Splunk для вирішення завдань кримінальної розвідки.
- 57.Використання Datasplloit для вирішення завдань кримінальної розвідки.
- 58.Здійснення картографування з використанням засобів Rigel компанії ECRI.
- 59.Здійснення картографування з використанням засобів CrimeStat.
- 60.Здійснення картографування з використанням засобів RICAS.
- 61.Вітчизняний досвід проведення аналітичної роботи.