МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки, факультет № 4

РОБОЧА ПРОГРАМА

навчальної дисципліни «*Поліцейська діяльність у кіберсфері*»
***вибіркових* компонент**
освітньої програми *першого* рівня вищої освіти

081 Право (протидія кіберзлочинності)

Харків 2019

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 19.09.2019 № 8

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 28.08.2019 № 7

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС _____
Протокол від 17.09.2019 № 9

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки
(*протокол від 27.08.2019 № 3*)

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;

Павликівський В.І., завідувач кафедри кримінально-правових дисциплін та адміністративного права Харківського університету, д.ю.н., доцент

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 8 Загальна кількість годин – 240 Кількість тем – 4	08 Право 081 Право бакалавр	Навчальний курс 4 Семестр 7 Види підсумкового контрою: - залік.
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання Лекції – 30; Практичні заняття – 70; Самостійна робота – 140; Індивідуальні завдання: Реферати – 1		

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Поліцейська діяльність у кіберсфері» є засвоєння курсантами особливостей використання комп'ютерних технологій працівниками поліції під час виявлення, попередження та розслідування злочинів.

Завданнями вивчення дисципліни «Поліцейська діяльність у кіберсфері» є дослідження принципів та методів протидії кіберзлочинам (визначення, класифікація, організаційні основи, нормативно-правова база застосування, типові схеми), ознайомлення з міжнародним досвідом протидії кіберзлочинності (особливості протидії кіберзлочинності у країнах з англо-саксонською та романо-германською системами права), засвоєння моделей поліцейської розвідки, методів і способів оперативного маскування у кіберсфері, набуття знань і навичок використання технологій під час попередження та розслідування кіберзлочинів.

Згідно з освітньою програмою здобувачі вищої освіти повинні:

знати:

- визначення, ознаки та класифікацію кіберзлочинів;
- нормативно-правову базу протидії кіберзллочинності;
- організаційну структуру протидії кіберзлочинності правоохоронним органами в Україні та за її межами;
- особливості організації і тактики оперативного маскування під час роботи в інформаційно-телекомунікаційних системах;
- моделі поліцейської розвідки;
- технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події;
- методи встановлення IP-адреси;

вміти:

- застосовувати норми законодавства у протидії кіберзлочинності;
- визначати методи протидії конкретним кіберзлочинам;
- використовувати зарубіжний досвід у протидії кіберзлочинності;
- застосовувати прийоми оперативного маскування у кіберсфері;
- здійснювати віддалений збір інформації про вузли комп'ютерної мережі;
- шукати інформацію про об'єкти в мережі;
- аналізувати профілі соціальних мереж та поштові повідомлення;
- встановлювати інформацію про фінансові інструменти;

бути ознайомленими

- з особливостями функціонування комп'ютерних мереж, веб-технологій, засобів комунікації, мережних засобів зберігання інформації, фінансових комп'ютерних технологій.

3. Програма навчальної дисципліни

Тема № 1. Засадничі принципи протидії кіберзлочинності.

Об'єкти та суб'єкти протидії кіберзлочинності. Організаційно-правові засади протидії кіберзлочинності. Міжнародний досвід протидії кіберзлочинності. Аналітична робота у протидії кіберзлочинності.

Тема № 2. Оперативне маскування у кіберсфері.

Поняття, суб'єкти та підстави застосування оперативного маскування. Забезпечення анонімності під час роботи в інформаційно-телекомунікаційних системах. Термінологічні особливості спілкування у кіберпросторі. Легендування профілів користувача для використання у кіберсфері.

Тема № 3. Кримінальна розвідка.

Поняття та зміст кримінальної розвідки (зарубіжний досвід). Розвідка з відкритих джерел (OSINT).

Тема № 4. Особливості використання технологій під час попередження та розслідування кіберзлочинів.

Комп'ютерні мережі та веб-технології. Засоби комунікації та мережні засоби зберігання інформації. Фінансові комп'ютерні технології. Технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події.

4. Структура навчальної дисципліни
4.1.1. 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 № 7							
Тема № 1 **Засадничі принципи протидії кіберзлочинності**	**32**	**6**		**6**		**20**	**Залік**
Тема № 2 **Оперативне маскування у кіберсфері**	**58**	**8**		**10**		**40**	
Тема № 3 **Кримінальна розвідка**	**62**	**8**		**14**		**40**	
Тема № 4 **Особливості використання технологій під час попередження та розслідування кіберзлочинів**	**88**	**8**		**40**		**40**	
Всього за семестр № 7:	**240**	**30**		**70**		**140**	

4.1.3. Питання, що виносяться на самостійне опрацювання

Завдання що виносяться на самостійну роботу курсанта (студента, слухача)	Література:
Тема № 1. Засадничі принципи протидії кіберзлочинності	
Самостійно дослідити нормативно-правові акти, як регламентують протидію кіберзлочинності	**1-105, Інтернет**
Дослідити схеми вчинення кіберзлочинів та запропонувати власні методи протидії ним	**1-105, Інтернет**
Підготувати реферат про досвід протидії кіберзлочинності в одній з країн, не відзначеній у лекційному курсі	**1-105, Інтернет**
Тема № 2. Оперативне маскування у кіберсфері	
Здійснити опрацювання підзаконної нормативно-правової бази застосування оперативного маскування	**1-105, Інтернет**
Встановити одну з ОС, орієнтованих на забезпечення анонімності в комп'ютерних мережах	**1-105, Інтернет**
Вивчити термінологію, яка застосовується у середовищі педофілів, кардерів та будь-якої іншої (за вибором) сфери злочинної діяльності, протидія якій охоплюється компетенцією кіберполіції	**1-105, Інтернет**
Заповнити таблицю «зручності» застосування різних сервісів для забезпечення анонімності	**1-105, Інтернет**
Вивчити методи деанонімізації особи в мережі	**1-105, Інтернет**
Тема № 3. Кримінальна розвідка	
Опрацювати британську систему оцінювання інформації та її джерел (5x5x5)	**1-105, Інтернет**
Опрацювати американську систему оцінювання інформації та її	**1-105, Інтернет**

		джерел (6х6)	
		Вивчити термінологію, яка застосовується у кримінальній розвідці	**1-105, Інтернет**
		Оцінити ефективність представлення інформації за допомогою різних діаграм в системі Anacapa	**1-105, Інтернет**
		Опрацювати методи стратегічного аналізу: SWOT, 5 сил Портера, конкурентний аналіз, техніку сценарію	**1-105, Інтернет**
		Скласти перелік актуальних джерел для здійснення OSINT у вітчизняному інформаційному просторі	**1-105, Інтернет**
		Вивчити способи аналізу даних в одній з соціальних мереж, яка не розглядається протягом теоретичного та практичного навчання	**1-105, Інтернет**
		Проаналізувати способи одержання інформації про викрадені речі	**1-105, Інтернет**
		Зібрати інформацію про себе в мережі Інтернет	**1-105, Інтернет**
		Дослідити методи встановлення IP-адрес користувачів месенджерів	**1-105, Інтернет**
		Засобами MS Excel створити відеодіаграму зростання злочинності в регіоні з прив’язкою до мапи	**1-105, Інтернет**
		Проаналізувати гаманець крипто валюти із застосуванням інструментів Maltego	**1-105, Інтернет**
		Вивчити методи аналітичного пошуку в системі RICAS	**1-105, Інтернет**
		Дослідити програмне забезпечення криміналістичного дослідження даних з протоколів роботи серверного обладнання	**1-105, Інтернет**
		Скласти порівняльну таблицю відомих інструментів кримінальної розвідки	**1-105, Інтернет**
	Тема № 4. Особливості використання технологій під час попередження та розслідування кіберзлочинів		
		Створити спеціальний сайт та розмістити його на хостингу з підтримкою PHP та FTP	**1-105, Інтернет**
		Вивчити способи налаштування VPN-з’єднання	**1-105, Інтернет**
		Проаналізувати способи одержання контактної інформації з мобільних пристроїв	**1-105, Інтернет**
		Дослідити програмне забезпечення криміналістичного дослідження даних з бортових комп’ютерів автомобілів	**1-105, Інтернет**
		Дослідити визначений навчальний ресурс на наявність вразливостей	**1-105, Інтернет**

5. Індивідуальні завдання

5.1.1. Теми рефератів

1. Система протидії кіберзлочинності у Франції.
2. Система протидії кіберзлочиинам в арабських країнах.
3. Африканський досвід протидії кіберзлочинам.
4. Протидія кіберзлочинам у країнах Латинської Америки.
5. Австралійський досвід протидії кіберзлочинності.
6. Набір сигнальних протоколів SS7 (Signaling System 7).
7. Методи імперсонації.
8. Особливості документування даних, одержаних з використанням комп’ютерних технологій.
9. Електронні платіжні системи.
10. Сучасні способи несанкціонованого зняття готівки з банкоматів.

5.1.2. Теми курсових робіт

1. Юрисдикція у кіберпросторі.
2. Міжнародна взаємодія у протидії кіберзлочинності.
3. Типові помилки і порушення законодавства, що допускаються при виявленні та документуванні кіберзлочинів.
4. Криміналістичне дослідження пристроїв на базі ОС Android.
5. Криміналістичне дослідження пристроїв на базі iOS.
6. Інноваційні методи віддаленого отримання інформації.
7. Інформаційно-аналітичне забезпечення протидії кіберзлочинності

5.1.3. Теми наукових робіт

1. Конвенція про кіберзлочинність як базовий документ для міжнародного співробітництва у сфері протидії кіберзлочинності в Європі.
2. Особливості придбання спеціальних технічних засобів для протидії кіберзлочинності за кордоном.
3. Нетрадиційні методи попередження та розслідування кіберзлочинів.
4. Збір (узагальнення, облік, збереження, використання) відомостей щодо власників (користувачів) «Інтернет-гаманців».
5. Адміністративна відповідальність за порушення у сфері інформаційних технологій.

6. Методи навчання

Лекції із застосуванням мультимедійного проектора; практичні заняття: моделювання ситуативних задач, дебати, тренінги, рольові та ігрові заняття, розв’язання задач тощо.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

1. Використання комп’ютерних технологій під час вчинення кримінальних правопорушень.
2. Поняття та способи вчинення кіберзлочинів.
3. Нормативно-правова база боротьби з кіберзлочинністю.
4. Суб’єкти боротьби з кіберзлочинністю.
5. Завдання підрозділів боротьби з кіберзлочинністю.
6. Функції підрозділів боротьби з кіберзлочинністю.
7. Типові схеми здійснення кіберзлочинів.
8. Визначення поняття «кіберпростір», його ознаки.
9. Вчинення злочинів через кіберпростір.
10. Питання визначення компетенції правоохоронних органів у кіберпросторі.
11. Шляхи конвергенції організованої злочинності та кіберпростору.
12. Цілодобова мережа для здійснення контактів з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення.

13. Український досвід регулювання питання здійснення оперативно-розшукових заходів шляхом використання кіберпростору.
14. Органи боротьби з кіберзлочинністю в різних країнах.
15. Боротьба зі злочинністю з використанням комп'ютерних технологій у російському законодавстві та в теорії оперативно-розшукової діяльності.
16. Інструменти здійснення оперативно-розшукових заходів через кіберпростір у США.
17. Зміст онлайнової секретної операції в США.
18. Правила онлайнових розслідувань США.
19. Боротьба з кіберзлочинністю у ФРН та загальний порядок здійснення проникнення за допомогою технічних засобів у інформаційно-технічні системи, що використовуються підозрюваним.
20. Використання комп'ютерних технологій в негласній роботі правоохоронних органів Великої Британії та КНР.
21. Поняття, суб'єкти та підстави застосування оперативного маскування.
22. Забезпечення анонімності під час роботи в інформаційно-телекомунікаційних системах.
23. Термінологічні особливості спілкування у кіберпросторі.
24. Легендування профілів користувача для використання у кіберсфері.
25. Поняття, структура та класифікація комп'ютерних мереж.
26. Адресація в комп'ютерних мережах.
27. Загальний порядок пошуку інформації правоохоронними органами про об'єкти в мережі.
28. Веб-сайти, дошки оголошень.
29. Комп'ютерні соціальні мережі.
30. Електронна пошта.
31. Мультимедійні засоби спілкування.
32. Загальна інформація про бази даних.
33. Хмарні сховища.
34. Peer-to-peer.
35. FTP та відеохостинги.
36. Електронні гроші та Інтернет орієнтовані платіжні системи.
37. Головні способи легалізації коштів.
38. Огляд стандартних засобів комп'ютерної техніки.
39. Огляд мобільних засобів комп'ютерної техніки із функцією телефону.
40. Огляд автомобільних засобів комп'ютерної техніки.
41. Особливості використання комп'ютерних технологій в негласній роботі Національної поліції України.
42. Сенс кримінальної розвідки.
43. Стратегії кримінальної розвідки.
44. Види кримінальної розвідки.
45. Стратегічна кримінальна розвідка.
46. Інструменти і методи стратегічної кримінальної розвідки.

47. Тактична кримінальна розвідка.
48. Інструменти і методи тактичної кримінальної розвідки.
49. Оперативна кримінальна розвідка.
50. Інструменти і методи оперативної кримінальної розвідки.
51. Засоби кримінальної розвідки.
52. Застосування методології Anacapa у кримінальній розвідці.
53. Етапи кримінальної розвідки.
54. Постановка завдань як етап здійснення кримінальної розвідки.
55. Збирання даних як етап здійснення кримінальної розвідки.
56. Оцінка даних як етап здійснення кримінальної розвідки.
57. Системи оцінки 4x4, 5x5, 6x6.
58. Обробка даних як етап здійснення кримінальної розвідки.
59. Аналіз даних як етап здійснення кримінальної розвідки.
60. Дерево зв'язків (link charting).
61. Дерево подій (event charting).
62. Дерево цінностей (commodity flow charting).
63. Дерево дій (activity charting).
64. Фінансове профілювання (financial profiling).
65. Частотний графік (frequency charting).
66. Кореляція даних (data correlation)
67. Мережний аналіз даних.
68. Особливості побудови діаграм за даними про телефонні з'єднання.
69. Розробка аналітичних висновків як етап здійснення кримінальної розвідки.
70. Види аналітичних висновків.
71. Зміст аналітичних висновків. Система запитань 5W+H.
72. Етапи проведення аналізу конкуруючих гіпотез.
73. Поширення інформації як етап здійснення кримінальної розвідки.
74. Повторний аналіз інформації.
75. Джерела відкритої інформації.
76. Пошук інформації про об'єкти в мережі.
77. Збирання інформації про мережі даних.
78. Аналіз профілів соціальних мереж.
79. Методи встановлення IP-адреси.
80. Аналіз заголовків електронних документів.
81. Аналіз метаданих.
82. Систематизація одержаної інформації.
83. Загальні інструменти для аналізу даних.
84. Сенс та завдання картографування злочинних проявів.
85. Інструменти картографічного профілювання.
86. Використання MS Excel для вирішення завдань кримінальної розвідки.
87. Використання IBM i2 для вирішення завдань кримінальної розвідки.
88. Використання Palantir для вирішення завдань кримінальної розвідки.
89. Використання Maltego для вирішення завдань кримінальної розвідки.

90. Використання Splunk для вирішення завдань кримінальної розвідки.
91. Використання Datasploit для вирішення завдань кримінальної розвідки.
92. Здійснення картографування з використанням засобів Rigel компанії ECRI.
93. Здійснення картографування з використанням засобів CrimeStat.
94. Здійснення картографування з використанням засобів RICAS.
95. Вітчизняний досвід проведення аналітичної роботи.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи оцінювання результатів навчання включають в себе поточний та підсумковий контролі.

Засобами оцінювання результатів навчання можуть бути екзамени (комплексні екзамени); тести; наскрізні проекти; командні проекти; аналітичні звіти, реферати, есе; розрахункові та розрахунково-графічні роботи; презентації результатів виконаних завдань та досліджень; завдання на лабораторному обладнанні, тренажерах, реальних об'єктах тощо; інші види індивідуальних та групових завдань.

Поточний контроль. До форм поточного контролю належить оцінювання:

- рівня знань під час семінарських, практичних, лабораторних занять;
- якості виконання самостійної роботи.

Поточний контроль здійснюється під час проведення семінарських, практичних та лабораторних занять і має на меті перевірку набутих здобувачем вищої освіти (далі – здобувач) знань, умінь та інших компетентностей з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну роботу виставляються в журналі обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (семінарські, практичні, лабораторні тощо); самостійна робота (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп’ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у формі, передбаченій в робочою програмою навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття

або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

$$\textit{Загальна кількість балів (перед підсумковим контролем)} = (\ \textit{Результат навчальних занять за семестр} + \textit{Результат самостійної роботи за семестр}\ ) / 2 * 10$$

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

$$\textit{Підсумкові бали навчальної дисципліни} = \textit{Загальна кількість балів (перед підсумковим контролем)} + \textit{Кількість балів за підсумковим контролем}$$

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\textit{Підсумкові бали навчальної дисципліни} = (\ \textit{Підсумкові бали за поточний семестр} + \textit{Підсумкові бали за попередній семестр}\ ) : 2$$

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на семінарських, практичних, лабораторних та інших аудиторних заняттях, самостійна*

робота, виконання індивідуальних творчих завдань) та підсумкового контролю. Кафедра визначає вимоги до здобувачів стосовно засвоєння змісту навчальної дисципліни, а саме: кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної роботи. Наприклад:

Робота під час навчальних занять	**Самостійна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, виконати практичне завдання тощо	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах		**Оцінка за національною шкалою**	**Оцінка**	
			Оцінка	**Пояснення**
12	**97-100**	Відмінно («зараховано»)	A	**«Відмінно»** – теоретичний зміст курсу засвоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
11	**94-96**			
10	**90-93**			
9	**85-89**	Добре («зараховано»)	B	**«Дуже добре»** – теоретичний зміст курсу засвоєний **цілком**, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома - трьома незначними помилками.
8	**80-84**			
7	**75 – 79**		C	**«Добре»** – теоретичний зміст курсу засвоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією – двома значними помилками.
6	**70-74**	Задовільно («зараховано»)	D	**«Задовільно»** – теоретичний зміст курсу засвоєний **частково**, але **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань містять **помилки,** робота з трьома значними помилками.
5	**65-69**			
4	**60-64**		E	**«Достатньо»** – теоретичний зміст курсу засвоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконана** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
3	**40–59**	Незадовільно («не	FX	**«Умовно незадовільно»** – теоретичний зміст курсу засвоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм навчання, навчальних завдань

2	**21-40**	зараховано»)		**не виконано**, або якість їхнього виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки.
1	**1–20**		F	**«Безумовно незадовільно»** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не сформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не приведе** до значного **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки.

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

1. Порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання : затверджений постановою Кабінету Міністрів України № 86 : від 28.01.2004 : [із змінами і доповненнями на 29.11.2018] // Офіційний вісник України. 2004. № 4 (13.02.2004) (частина 1). Ст. 167.
2. Gibson W. Neuromancer. London: HarperCollins, 1994. 271 p.
3. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом в 2005–2006 роках : затверджені наказом Держфінмоніторингу України : від 22.12.2006 № 265 // Українська інвестиційна газета. 2007. № 44, 11.
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 // Відомості Верховної Ради України. 2017. № 45 (10.11.2017). Ст. 403.
5. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. № 4 (31). С. 215–219.
6. Золотий щит. URL: : http://ru.wikipedia.org/wiki/Золотий_щит (дата звернення: 10.12.2018).
7. Minnesota v. Granite Gate Resorts, Inc., 1996 WL 767431 (Minn. Dist. Ct. 1996) / Court File No. C6-95-7227. URL: : http://www.loundy.com/CASES/Minn_v_Granite_Gate.html (дата звернення: 10.12.2018).
8. Додонов В. В. Сравнительное уголовное право. Общая часть: монография / под общ. ред. и науч. ред. С. П. Щербы. М. : Юрлитинформ, 2009. 448 с.
9. Науково-практичний коментар до Кримінального кодексу України: за станом законодавства і Постанов Пленуму Верховного Суду України на 1 грудня 2001 р. / за ред. С.С. Яценка. К. : А.С.К., 2002. 906 с.
10. Жителя Сочи довели до суицида с помощью сайта «Одноклассники»(22.12.2011). URL: www.securitylab.ru/news/412942.php (дата звернення: 10.12.2018).
11. Robertson N. Documents reveal al Qaeda’s plans for seizing cruise ships, carnage in Europe / N. Robertson, P. Cruickshank, T. Lister.

URL: http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/?hpt=hp_c1 (дата звернення: 10.12.2018).

12. Shelley L. Organized Crime, Terrorism and Cybercrime / перевод исследователя ВЦИОП Т. Л. Тропиной URL: http://www.crime.vl.ru/index.php?p=928&more=1&c=1&tb=1&pb=1 (дата звернення: 10.12.2018).

13. СБУ разыскивает Интернет-рекетиров. URL: http://podrobnosti.ua/podrobnosti/2012/02/13/820044.html (дата звернення: 10.12.2018).

14. Современные технологии в наркобизнесе / А.И. Гуров, Т.М. Виноградская, Б.Ф. Калачёв. URL: http://www.narkotiki.ru/mir_5553.html (дата звернення: 10.12.2018).

15. Кузнецов А.В. Доклад на VII Международной конференции «Право и Интернет». URL: http://www.securitylab.ru/opinion/241966.php (дата звернення: 10.12.2018).

16. Осипенко А.Л. О некоторых особенностях раскрытия сетевых компьютерных преступлений. *Научный портал МВД России*. 2010. № 2(10). С. 42-47.

17. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. URL: http://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення: 12.06.2017).

18. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015. К. : Національна поліція України, 2015. 9 с.

19. Кібербанди стають схожі на високоорганізовані синдикати. URL: http://unian.net/ukr/news/news-369195.html.

20. Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers [Електронний ресурс]. – 25 р. – Режим доступу : https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf.

21. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби / Н. В. Савчук // Теоретичні та прикладні питання економіки : збірник наукових праць. – 2009. – № 19. – С. 338-342.

22. Quick Facts. URL: http://www.fbi.gov/about-us/quick-facts (дата звернення: 10.12.2018).

23. Современные технологии в наркобизнесе / А.И. Гуров, Т.М. Виноградская, Б.Ф. Калачёв. URL: http://www.narkotiki.ru/mir_5553.html (дата звернення: 10.12.2018).

24. Зубченко Л.А. Информационные войны и киберпреступность. URL: http://www.bankir.ru/analytics/refer/84/4616 (дата звернення: 10.12.2018).

25. В Британии появятся киберполисмены / Би-би-си – Русская служба. URL: http://news.bbc.co.uk/low/russian/uk/newsid_1284000/1284044.stm (дата звернення: 10.12.2018).

26. National Cyber Crime Unit. URL: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit (дата звернення: 10.12.2018).

27. XML Data Corpus : Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat. WP4. D.4.1 / Ioannis Klapaftis, Suresh Manandhar, Shailesh Pandey [European Seventh Framework Programme FP7-218086-Collaborative Project] ; INDECT Consortium. 2009. 41 p.

28. Lorch S. Расследование случаев распространения детской порнографии в Интернете. *Інформаційний бюлетень*. К. : МНДЦ, 2004. № 5. С. 145-157.

29. Оперативно-розыскная деятельность : учебник / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова ; 2-е изд., доп. и перераб. М : ИНФРА-М, 2004. 848 с.

30. Теория оперативно-розыскной деятельности / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. М. : Норма, 2006. 368 с. (Краткие учебные курсы юридических наук).

31. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: монография. М.: Норма, 2004. 32 с.

32. МВД создаст новые IT подразделения. URL: http://www.securitylab.ru/news/420008.php (дата звернення: 10.12.2018).

33. Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=110026 (дата звернення: 10.12.2018).

34. Осипенко А.Л. О некоторых особенностях раскрытия сетевых компьютерных преступлений. *Научный портал МВД России*. 2010. № 2(10). С. 42-47.

35. National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders Washington, D.C. : U.S. Department of Justice, National Institute of Justice, 2001. NCJ 187736.

36. Макнамара Д. Секреты компьютерного шпионажа : Тактика и контрмеры / пер с англ. ; под ред. С.М. Молявко. М. : БИНОМ. Лаборатория знаний, 2004. 536 с.

37. The Attorney General’s Guidelines for Domestic FBI Operations. September 29, 2008.

38. The Attorney General’s Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.

39. FBI: Woman Posted Craigslist and Seeking Killer for Lover’s Wife. URL: http://www.usatoday.com/news/nation/2008-01-26-craigslist-hitman_N.htm (дата звернення: 10.12.2018).

40. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.

41. Leyden John. UK cops set up new £30m bases to nail cybercrooks. URL: http://www.theregister.co.uk/2012/02/09/regional_cyber_hubs_fight_e_crime/ (дата звернення: 10.12.2018)

42. Ущерб Великобритании от киберпреступности составил $43 млрд. URL: http://www.pravo.ru/interpravo/news/view/48812/ (дата звернення: 10.12.2018).

43. Practice Advice on Tackling Commercial Cannabis Cultivation and Head Shops. Bedfordshire: ACPO NPIA, 2009. 57 p.

44. Германия начнет войну против киберпреступников. URL: http://news.mail.ru/politics/5047697/ (дата звернення: 10.12.2018).

45. Немецкая полиция может получить разрешение на тайный взлом компьютеров. URL: http://www.zakon.kz/international_news/109665-nemeckaja-policija-mozhet-poluchit.html (дата звернення: 10.12.2018).

46. Schaar P. Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden. 5 p. URL: http://www.ccc.de/system/uploads/122/original/Schaar-Staatstrojaner.pdf/ (дата звернення: 10.12.2018).

47. Син Янь. Организованная преступная деятельность в Китайской Народной Республике и общеметодические основы её расследования [Текст]: дисс. на соиск. уч. степени канд. юрид. наук : спец. 12.00.09 – уголовный процесс, криминалистика и судебная экспертиза; оперативно-розыскная деятельность. М., 2004. 187 с.

48. Comissioner’s Operational Priorities 2018. URL: https://www.police.gov.hk/ppp_en/01_about_us/cop2018.html (дата звернення: 10.12.2018).

49. 互联网信息服务管理办法（国务院令第292号）. URL: http://www.mps.gov.cn/n16/n1282/n3493/n3778/n492863/493177.html (дата звернення: 10.12.2018).

50. Ян Вэй Фэн. Расследование компьютерных преступлений в Китайской народной республике: криминалистические аспекты : автореф. дисс. на соиск. уч. степени канд. юрид. наук: спец. 12.00.09 – уголовный процесс, криминалистика и судебная экспертиза; оперативно-розыскная деятельностьн. М., 2006. 23 с.

51. Monette H. Herrera NBI creates crime unit to capture cybercrime violators URL: http://www.pia.gov.ph/news/index.php?article=1901353660025 (дата звернення: 10.12.2018).

52. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 с.

53. 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: 10.12.2018).

54. The National Criminal Intelligence Sharing Plan / Department of Justice. 2003. 54 с. URL: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf (дата звернення: 10.12.2018).

55. 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.

56. 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. pp. 433-442.

57. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк : Управление Организации Объединенных Наций по наркотикам и преступности, 2010. 36 с. URL: https://www.unodc.org/pdf/criminal_justice/10-52547_1_Policing_4_ebook.pdf (дата звернення: 10.12.2018).

58. 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.

59. Богинский О. В. Некоторые методы, применяемые для подготовки аналитических выводов, в рамках института криминальной разведки. *Legea si Viata*. 2018. № 3. С. 11-15.

60. Информационные технологии в деятельности подразделений экономической безопасности и противодействия коррупции: монография / А. А. Крылов, В. Н. Анищенко, Э. А. Васильев, С. В. Дегтярев, Е. Н. Зарубина, С. В. Маликов, Р. С. Мацкевич, В. О. Морар, А. Л. Ситковский. М. : ФГКУ «ВНИИ МВД России», 2015. 304 с.

61. Ferrara E., De Meo P., Catanese S., Fiumara G. Visualizing criminal networks reconstructed from mobile phone records. In: Hypertext 2014 Extended Proceedings: Late-breaking Results, Doctoral Consortium and Workshop Proceedings of the 25th ACM Hypertext and Social Media Conference (Hypertext 2014), Santiago, Chile, September 1-4, 2014. URL: https://arxiv.org/abs/1407.2837 (дата звернення: 22.06.2017).

62. Duijn P., Klerks P. Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement, *Networks and Network Analysis for Defence and Security,* Lecture Notes in Social Networks. 2014. P. 121-159. DOI: 10.1007/978-3-319-04147-6_1.

63. Ribaux O., Margot P. Case based reasoning in criminal intelligence using forensic case data. *Science & Justice*. 2003. № 3. pp. 135-143.

64. Rossy Q, Ribaux O. A collaborative approach for incorporating forensic case data into crime investigation using criminal intelligence analysis and visualisation. *Science & Justice*, 2014. № 54. pp. 146-153.

65. Xu J. J., Chen H. Fighting organized crimes: using shortest-path algorithms to identify associations in criminal networks. *Decision Support Systems*. 2004. № 38(3). pp. 473-487 (DOI:10.1016/S0167-9236(03)00117-9).

66. Berlusconi G., Calderoni F., Parolini N., Verani M, Piccardi C. Link Prediction in Criminal Networks: A Tool for Criminal Intelligence Analysis. *PloS one*. 2016. – № 11(4). :e0154244. DOI:10.1371/journal.pone.0154244.

67. Манжай О. В., Осятинська І. А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами // Актуальні

питання розслідування кіберзлочинів: матеріали міжнарод. наук.-практ. конф. (Харків, 10 грудня 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. Х : ХНУВС, 2013. С. 256-258.

68. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (Дата звернення: 22.09.2017).

69. Ташмагамбетов А. М. Оперативно-розыскные мероприятия с использованием социальных сетей: опыт Великобритании и Республики Казахстан. *Наука и бизнес: пути развития*. 2013. № 11 (29). С. 129-133.

70. Greenemeier L. A new set of search tools called Memex, developed by DARPA, peers into the “deep Web” to reveal illegal activity. URL: https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/ (Дата звернення: 22.09.2017).

71. Соцсети позволяют легко найти номера мобильных телефонов многих пользователей. URL: http://www.securitylab.ru/news/440882.php (Дата звернення: 22.09.2017).

72. Unique in the Crowd: The privacy bounds of human mobility / Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, Vincent D. Blondel. URL: http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html (Дата звернення: 22.09.2017).

73. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (Проект): навчальний курс / [В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков]. К., 2015. 158 с.

74. Інтернет-технології URL: https://uk.wikipedia.org/wiki/Інтернет-технології (дата звернення: 10.12.2018).

75. Веб-сайт URL: https://uk.wikipedia.org/wiki/Веб-сайт (дата звернення: 10.12.2018).

76. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.12.2018).

77. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.12.2018).

78. 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.

79. Європейська конвенція про взаємну допомогу у кримінальних справах: від 20.04.1959: ратифікована Верховною радою України 16.01.1998. *Офіційний вісник України*. 2004. № 26. С. 231. Ст. 173.

80. Skype URL: https://uk.wikipedia.org/wiki/Skype (дата звернення: 10.12.2018).

81. Viber URL: https://uk.wikipedia.org/wiki/Viber (дата звернення: 10.12.2018).

82. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності: монографія. Харків : Золота миля, 2012. 620 с.

83. Відеохостинг URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 10.12.2018.

84. Про платіжні системи та переказ коштів в Україні: закон України від 05.04.2001 [із змінами і доповненнями на 24.11.2018]. *Офіційний вісник України*. 2001. № 20 (01.06.2001). ст. 828.

85. Положення про електронні гроші в Україні, затверджене постановою Правління Національного банку України від 04.11.2010 № 481 [із змінами і доповненнями на 12.09.2018]. *Офіційний вісник України*. 2010. № 100 (04.01.2011). ст. 3571.

86. Методика розкриття злочинів, вчинених у сфері функціонування платіжних карток та електронних розрахунків: наук.-метод. рек. / О. І. Безпалова, Д. Т. Карпізін, В. В. Носов, О. В. Манжай, В. І. Стреляний. Х. : Харк. нац. ун-т. внутр. справ. 2013. 79 с.

87. Криптовалюта URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 10.12.2018).

88. Незаконні дії з банківськими платіжними картками: методичні рекомендації. К. : МВС України, 2013. 28 с.

89. WebMoney URL: https://uk.wikipedia.org/wiki/WebMoney (дата звернення: 10.12.2018).

90. Дахно І. І. Зовнішньоекономічний менеджмент. К. : Центр учбової літератури, 2012. 568 с.

91. 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.

92. Handbook of Digital Forensics and Investigation / edited by Eoghan Casey. Elsevier Academic Press, 2010. 567 p.

93. Петрович Л., В'ятов Н. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України. К. : Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні»), 2014. 60 с.

94. Літвінов М. Ю. Проблемні питання фіксації комп'ютерних слідів під час здійснення огляду // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., м. Харків, 23 квіт. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ ; Незалеж. асоц. банків України, Харк. банк. союз. регіон. представник НАБУ. Х. : ХНУВС, 2013. С. 20-23.

95. Mccoy M. Collection and Preservation of Digital Evidence / Mark Mccoy, Rachael Elliott // The Detective's Handbook / edited by John A. Eterno, Cliff Roberson. London, New-York : CRC Press, 2015. 358 с.

96. TRIM. URL: https://ru.wikipedia.org/wiki/TRIM (дата звернення: 10.12.2018).

97. Манжай О. В., Бучак Т. А. Методика контекстного пошуку документів, які оброблялися в інформаційно-телекомунікаційній системі, в рамках проведення контрольних заходів по перевірці стану інформаційної безпеки організації // Матеріали науково-практ. конференції «Інформатизація вищих навчальних закладів МВС України». Х. : Вид-во Харківського нац. ун-ту внутр. справ. 2008. С. 151-153.

98. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.

99. Про телекомунікації : закон України від 18.11.2003 : [із змінами і доповненнями на 04.11.2018]. *Офіційний вісник України*. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644.

100. National Intelligence Model: Code of Practice. – CENTREX, 2005. 14 с. URL: http://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf (дата звернення: 10.12.2018).

101. Про кіберзлочинність : конвенція Ради Європи : від 07.09.2005 : ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.12.2018).

102. Кибермaньячка окажется на скамье подсудимых (17.05.2008). URL: https://www.nedelia.lt/sama-zhizn/2685-novyjj-vid-prestuplenija-kibermanjaki.html (дата звернення: 10.12.2018).

103. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.

104. Вирок Кіровського районного суду м. Кіровограда від 06.03.2014 : Справа № 404/10729/13-к URL: http://www.reyestr.court.gov.ua/Review/37493964 (дата звернення: 10.12.2018).

105. MD5. URL: https://ru.wikipedia.org/wiki/MD5 (дата звернення: 10.12.2018).