МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності, факультет № 4

РОБОЧА ПРОГРАМА

навчальної дисципліни «*Поліцейська діяльність у кіберсфері*»
обов'язкових* компонент для спеціальності «Кібербезпека» та *вибіркових
компонент для спеціальності «Право»
освітньої програми *першого* рівня вищої освіти

125 Кібербезпека, 081 Право (поліцейські)

Харків 2023

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

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.08.2023 № 8

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

Розглянуто на засіданні кафедри протидії кіберзлочинності (*протокол від 15.08.2023 № 19*

Розробник:
Завідувач кафедри протидії кіберзлочинності, к.ю.н., професор Манжай О.В.

Рецензенти:

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

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

1. Опис навчальної дисципліни
Спеціалізація «протидія кіберзлочинності»

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти	Характеристика навчальної дисципліни
125 Кібербезпека Кількість кредитів ECTS – 6 Загальна кількість годин – 180 Кількість тем – 2 081 Право Кількість кредитів ECTS – 3 Загальна кількість годин – 90 Кількість тем – 1	12 Інформаційні технології 125 Кібербезпека 08 Право 081 Право бакалавр	125 Кібербезпека Навчальний курс 3, 4 Семестри 6, 7 Види підсумкового контрою: - залік, екзамен. 081 Право Навчальний курс 4 Семестр 7 Вид підсумкового контрою: - залік.
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання 125 Кібербезпека Лекції – 24; Лабораторні заняття – 36; Практичні заняття – 0; Самостійна робота – 120; 081 Право Лекції – 8; Семінарські заняття – 8; Практичні заняття – 28; Самостійна робота – 44; Індивідуальні завдання: Реферати – 1		

2. Мета та завдання навчальної дисципліни

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

Міждисциплінарні зв'язки: «Безпека інформаційно-комунікаційних систем», «Оперативно-розшукова діяльність», «Цифрова криміналістика».

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.

Програмні компетентності (125 Кібербезпека):

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційних технологій (кібербезпека), що передбачає ідентифікацію та використання інформації для прийняття рішень	
Загальні компетентності (ЗК)	ЗК.7	Знання та розуміння предметної області та розуміння професії

Програмні компетентності (081 Право):

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі професійної правничої діяльності або у процесі навчання, що передбачає застосування правових доктрин, принципів і правових інститутів і характеризується комплексністю та невизначеністю умов	
Загальні компетентності (ЗК)	ЗК.2	Здатність застосовувати знання у практичних ситуаціях
	ЗК.6	Навички використання інформаційних і комунікаційних технологій
Спеціальні (фахові, предметні) компетентності (СК)	СК.8	Здатність і розуміння особливостей реалізації та застосування норм матеріального і процесуального права
	СК.13	Здатність до критичного та системного аналізу правових явищ і застосування набутих знань у професійній діяльності

3. Програма навчальної дисципліни

Тема № 1. Засадничі принципи протидії кіберзлочинності та інструментарій поліції у кіберсфері.

Об'єкти та суб'єкти протидії кіберзлочинності. Організаційно-правові засади протидії кіберзлочинності. Міжнародний досвід протидії кіберзлочинності. Територіальний моніторинг інформаційних ресурсів. Використання систем штучного інтелекту в поліцейській діяльності.

Тема № 2. Об'єкти уваги та особливості використання технологій під час попередження та розслідування кіберзлочинів.

Мережні технології. Мережні засоби зберігання інформації. Фінансові комп'ютерні технології. Технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події. Аналіз електронних даних по наркозлочинах, які вчиняються з використанням можливостей кіберсфери.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами за спеціальністю «Кібербезпека», спеціалізація «поліцейські» (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 № 6							
Тема № 1 **Засадничі принципи протидії кіберзлочинності та інструментарій поліції у кіберсфері**	**90**	**20**			**24**	**46**	**Залік**
Всього за семестр № 6:	**90**	**20**			**24**	**46**	
Семестр № 7							
Тема № 2 **Об'єкти уваги та особливості використання технологій під час попередження та розслідування кіберзлочинів**	**90**	**20**			**26**	**44**	**Екзамен**
Всього за семестр № 7:	**90**	**20**			**26**	**44**	

«Право», спеціалізація «поліцейські» (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 та інструментарій поліції у кіберсфері**	**90**	**8**	**8**	**28**		**46**	**Залік**
Всього за семестр № 7:	**90**	**8**	**8**	**28**	**0**	**46**	

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література:
Тема № 1. Засадничі принципи протидії кіберзлочинності та інструментарій поліції у кіберсфері	
Самостійно дослідити нормативно-правові акти, як регламентують протидію кіберзлочинності	**1-77, Інтернет**
Дослідити схеми вчинення кіберзлочинів та запропонувати власні методи протидії ним	**1-77, Інтернет**
Підготувати реферат про досвід протидії кіберзлочинності в одній з країн, не відзначеній у лекційному курсі	**1-77, Інтернет**
Тема № 2. Об'єкти уваги та особливості використання технологій під час попередження та розслідування кіберзлочинів	
Створити спеціальний сайт та розмістити його на хостингу з підтримкою PHP та FTP	**1-77, Інтернет**
Вивчити способи налаштування VPN-з'єднання	**1-77, Інтернет**
Проаналізувати способи одержання контактної інформації з мобільних пристроїв	**1-77, Інтернет**
Дослідити програмне забезпечення криміналістичного дослідження даних з бортових комп'ютерів автомобілів	**1-77, Інтернет**
Дослідити визначений навчальний ресурс на наявність вразливостей	**1-77, 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; лабораторні та 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. Створення профілів користувача для використання у кіберсфері.

25. Загальний порядок пошуку інформації правоохоронними органами про об'єкти в мережі.

26. Поняття, структура та класифікація комп'ютерних мереж.

27. Адресація в комп'ютерних мережах.

28. Загальний порядок пошуку інформації правоохоронними органами про об'єкти в мережі.

29. Документування інформації з вебсайтів та дощок оголошень.

30. Документування інформації з комп'ютерних соціальних мереж.

31. Встановлення відправника електронних поштових повідомлень.

32. Емейл-трекінг.

33. Види мультимедійних засобів спілкування.

34. Ідентифікація володільців облікових записів мультимедійних засобів спілкування.

35. Тимчасове збереження даних.

36. Загальна інформація про бази даних.

37. Банки даних Національної поліції України.

38. Хмарні сховища.

39. Peer-to-peer.

40. FTP та відеохостинги.

41. Електронні гроші та Інтернет орієнтовані платіжні системи.

42. Головні способи легалізації коштів.

43. Огляд стандартних засобів комп'ютерної техніки.

44. Огляд мобільних засобів комп'ютерної техніки із функцією телефону.

45. Огляд автомобільних засобів комп'ютерної техніки.

46. Особливості використання комп'ютерних технологій в негласній роботі Національної поліції України.

47. Системи штучного інтелекту в роботі поліції.

48. Протидія наркозлочинам у кіберсфері.

49. Моніторинг мережних ресурсів.

50. Способи ідентифікації правопорушника у кіберсфері.

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 зараховано»)	FX	**«Умовно незадовільно»** – теоретичний зміст курсу засвоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм навчання, навчальних завдань **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.
2	**21-40**			
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.

3. Рекомендована література (основна, допоміжна),

інформаційні ресурси в Інтернеті

Основна

1. Апетик А. М., Дьякова А. Д., Ковальова О. В., Козлова А. Г., Манжай О. В., Мердова О. М., Мілорадова Н. А., Пашко Н. А., Юртаєва К. В., Філоненко В. Підготовка поліцейських підрозділів превентивної діяльності, слідства, та дізнання, кіберполіцейських з питань убезпечення дітей у кіберпросторі: навчально-методичний посібник / за заг. ред. Т. В. Журавель, О. В. Ковальової. Київ: ГО Волонтер, 2023.

2. 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.

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

4. Манжай О. В. Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 178–180.

5. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.

6. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.

8. Реєстр методик проведення судових експертиз. URL: http://rmpse.minjust.gov.ua (дата звернення: 13.02.2023).

9. Особливості розслідування кримінальних правопорушень, пов'язаних із доведенням до самогубства неповнолітніх із використанням соціальних мереж в Інтернеті: науково-методичні рекомендації / О.В. Манжай, В.В. Кікінчук, В.В. Корнієнко, В.С. Гнатенко, О.М. Рвачов. Х. : ХНУВС, 2022. 57 с.

10. Методика розслідування створення та поширення контенту з вмістом дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій: науково-методичні рекомендації / С.О. Книженко, О.В. Салманов, О.В. Манжай, В.В. Кікінчук, В.В. Романюк. Х. : ХНУВС, 2022. 68 с.

11. Пошук та фіксація фактичних даних про протиправні діяння, які вчинені з використанням інформаційно-телекомунікаційних систем або технологій при розслідуванні фактів збуту наркотичних засобів: науково-

методичні рекомендації / В.В. Кікінчук, Т.П. Матюшкова, А.В. Піддубна, О.В. Манжай, В.В. Носов. Х. : ХНУВС, 2022. 69 с.

12. Носов В. В., Манжай І. А. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. *Право і безпека*. 2021. № 1(80). С. 93-100 (DOI: 10.32631/pb.2021.1.13).

13. Носов В. В., Манжай О. В., Панченко Є. В. Аналіз етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень. *Право і безпека*. 2022. № 4(87). pp. 108-124 (DOI: https://doi.org/10.32631/pb.2022.4.09).

14. Носов В. В., Манжай О. В., Ковтун В.О. Техніко-криміналістичні та організаційні аспекти роботи з криптовалютою Monero. *Право і безпека*. 2023. № 3(90). С. 102-125 (DOI: https://doi.org/10.32631/pb.2023.3.9).

15. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT) ; Чинний від 2019-01-01. Київ : УкрНДНЦ, 2018. VI, 31 с. : рис., табл. (Національний стандарт України).

16. 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: 10.05.2022).

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

18. Про електронні комунікації : Закон України від 16.12.2020 : [із змінами і доповненнями]. Офіційний вісник України. 2021. № 6 (21.01.2021). Ст. 306.

Допоміжна

19. 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.

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

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

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

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

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

Інформаційні ресурси в Інтернеті

25. Веб-сайт URL: https://uk.wikipedia.org/wiki/Веб-сайт (дата звернення: 10.05.2023).

26. 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: 10.05.2023).

27. Відеохостинг URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 10.05.2023).

28. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.05.2023).

29. Інтернет-технології URL: https://uk.wikipedia.org/wiki/Інтернет-технології (дата звернення: 10.05.2023).

30. Криптовалюта URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 10.05.2023).

31. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (Дата звернення: 22.09.2023).

32. cyberpolice.gov.ua.

33. hackthebox.eu.

34. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.05.2023).

35. TRIM. URL: https://ru.wikipedia.org/wiki/TRIM (дата звернення: 10.05.2023).

36. Viber URL: https://uk.wikipedia.org/wiki/Viber (дата звернення: 10.05.2023).