



МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх
справ

Факультет № 4

Кафедра протидії кіберзлочинності

Факультет № 6

Кафедра кібербезпеки та DATA-технологій

ЗАТВЕРДЖЕНО

На спільному засіданні кафедри
протидії кіберзлочинності факультету
№ 4 та кафедри кібербезпеки та
DATA-технологій факультету №6
протокол № 2 від 22 червня 2023 р.
Завідувач кафедри
протидії кіберзлочинності
Олександр МАНЖАЙ

ПОЛІЦЕЙСЬКА ДІЯЛЬНІСТЬ У КІБЕРСФЕРІ (ОК.04, ВК.15)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кафедра протидії кіберзлочинності (https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	kaf-itk@univd.edu.ua
ЛЕКТОР (ЛЕКТОРИ)	
	Манжай Олександр Володимирович, завідувач кафедри протидії кіберзлочинності факультету № 4, к.ю.н., професор moj@univd.edu.ua Лекційний потік: факультет № 4, шифр навчальних груп Ф4-302, 401
Назва освітньо-професійної програми	Кібербезпека (поліцейські) Cybersecurity (Police Officers) Право (поліцейські) Law (Police Officers)

Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень та перший цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології 08 Право
Спеціальність	125 Кібербезпека 081 Право
Статус дисципліни	Обов'язкова компонента освітньо-наукової програми для спеціальності «Кібербезпека», вивчається в 6,7 семестрі III-IV курсу навчання Вибіркова компонента освітньо-наукової програми для спеціальності «Право», вивчається в 7 семестрі IV курсу навчання
Мета вивчення дисципліни	<p>Навчити здобувачів вищої освіти особливостям використання комп'ютерних технологій працівниками поліції під час виявлення, попередження та розслідування кримінальних правопорушень.</p> <p>Виробити вміння щодо: застосовування норм законодавства у протидії кіберзлочинності; визначення методів протидії конкретним кіберзлочинам; застосування зарубіжного досвіду протидії кіберзлочинності; здійснення віддаленого збору інформації про вузли комп'ютерної мережі; пошуку інформації про об'єкти в мережі; аналізу профілів соціальних мереж та поштових повідомлень; встановлення інформації про фінансові інструменти.</p> <p>Сформувати у здобувачів вищої освіти знання, уміння і навички щодо функціонування комп'ютерних мереж, вебтехнологій, засобів комунікації, мережних засобів зберігання інформації, фінансових комп'ютерних технологій. функціонування комп'ютерних мереж, вебтехнологій, засобів комунікації, мережних засобів зберігання інформації, фінансових комп'ютерних технологій.</p>
Завдання вивчення дисципліни	Знати визначення, ознаки та класифікацію кіберзлочинів; нормативно-правову базу протидії кіберзлочинності; організаційну структуру протидії кіберзлочинності правоохоронними органами в Україні та за її межами; особливості організації і тактики оперативного маскування під час роботи в інформаційно-телекомунікаційних системах;

	<p>моделі поліцейської розвідки; технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події; методи встановлення IP-адреси.</p> <p>Розуміти правові засади організації та координації дій органів державної влади з протидії кримінальній протиправності у кіберсфері. Вміти орієнтуватися у проблемах міжнародного співробітництва у протидії кіберзлочинності.</p> <p>Упевнено застосувати понятійно-категоріальний апарат, юридичну практику для правозастосовної діяльності, в т.ч. правові позиції Європейського суду з прав людини, Верховного Суду України. Готувати необхідні процесуальні документи.</p> <p>Упевнено застосувати понятійно-категоріальний апарат, юридичну практику для правозастосовної діяльності, в т.ч. правові позиції Європейського суду з прав людини, Верховного Суду України. Готувати необхідні процесуальні документи.</p>
Обсяг дисципліни в кредитах ECTS/годинах для спеціальності «Кібербезпека»	6 кредитів ECTS (загальний обсяг - 180 год.)
	аудиторна робота: 90 год., з них:
	лекції: 40 год.
	лабораторні заняття: 50 год.
	самостійна робота: 90 год.
Обсяг дисципліни в кредитах ECTS/годинах для спеціальності «Право»	3 кредити ECTS (загальний обсяг - 90 год.)
	аудиторна робота: 44 год., з них:
	лекції: 8 год.
	семінарські заняття: 8 год.
	практичні заняття: 28 год
	самостійна робота: 46 год.
Форми та види проведення навчальних занять	<p>Форма навчання – денна.</p> <p>Види навчальних занять: лекції, семінарські, практичні, лабораторні, самостійна робота.</p>
Самостійна робота	Опрацювання рекомендованої літератури, підготовка тез доповідей до конференцій
Необхідне обладнання	Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Індивідуальні завдання	Наукові доповіді, реферати

Мова викладання	Українська
Контроль	Поточний та підсумковий контроль Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, рефератів; підготовка рефератів та доповідей, тестування, виконання самостійних робіт, захист лабораторних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Підсумковий контроль: залік, екзамен.
Інтегральна компетентність, загальні компетентності, спеціальні (фахові) компетентності	<p>Спеціальність «Кібербезпека» Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов</p> <p>ЗК.7 Знання та розуміння предметної області та розуміння професії</p> <p>Спеціальність «Право» 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</p> <p>ЗК.2 Здатність застосовувати знання у практичних ситуаціях</p> <p>ЗК.6 Навички використання інформаційних і комунікаційних технологій</p> <p>СК.8 Здатність і розуміння особливостей реалізації та застосування норм матеріального і процесуального права</p> <p>СК.13 Здатність до критичного та системного аналізу правових явищ і застосування набутих знань у професійній діяльності</p>
ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ	
<p>ТЕМА № 1. Засади протидії кіберзлочинності та інструментарій поліції у кіберсфері</p> <p>Об'єкти та суб'єкти протидії кіберзлочинності. Організаційно-правові засади протидії кіберзлочинності. Міжнародний досвід протидії кіберзлочинності. Територіальний моніторинг інформаційних ресурсів. Використання систем</p>	

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.	
Спеціальність «Кібербезпека» Програмні результати навчання (ПРН)	ПРН 7 діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки ПРН 9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки ПРН 22 застосовувати національні та міжнародні регулюючі акти у сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів ПРН 23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах ПРН 24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових) ПРН 25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів ПРН 26 впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-

	телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем ПРН 30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем ПРН 42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки	
Спеціальність «Право» Програмні результати навчання (ПРН)	ПНР 3 Проводити збір і інтегрований аналіз матеріалів з різних джерел ПНР 8 Використовувати різноманітні інформаційні джерела для повного та всебічного встановлення певних обставин ПНР 15 Вільно використовувати для професійної діяльності доступні інформаційні технології і бази даних	
Критерії оцінювання результатів навчання	Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю: - поточний контроль - 50 балів; - підсумковий контроль - 50 балів. Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: реферати, програми (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5. Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (заліку, екзамені).	
ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS		
Оцінка в	Оцінка за	Оцінка за шкалою ECTS

балах	національною шкалою	Оцінка	Пояснення
97-100	Відмінно ("зараховано")	А	„Відмінно” – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85-89	Добре ("зараховано")	В	„Дуже добре” – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.
80-84			
75-79		С	„Добре” – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі 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.
70-74	Задовільно ("зараховано")	D	„Задовільно” – теоретичний зміст курсу освоєний не повністю, 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.
65-69			

60-64		Е	„Достатньо” – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального, робота, що задовольняє мінімуму критеріїв оцінки.
40-59	Незадовільно („не зараховано”)	FX	„Умовно незадовільно” – теоретичний зміст курсу освоєний 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
21-40			
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 значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

Перелік питань, 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.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно-правові акти:

1. 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.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради України*. 2017. № 45 (10.11.2017). Ст. 403.
3. 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).
4. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.
5. Про електронні комунікації : Закон України від 16.12.2020 : [із змінами і доповненнями]. Офіційний вісник України. 2021. № 6 (21.01.2021). Ст. 306.
6. 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.
7. 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.
8. 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.

Основна література:

9. 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. Ковальнової. Київ: ГО Волонтер, 2023.
10. 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.

11. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.
12. 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.
13. 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.
14. 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.
15. 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).
16. 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>).
17. 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>).

Додаткова література:

18. 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).
19. Реєстр методик проведення судових експертиз. URL: <http://rmpse.minjust.gov.ua> (дата звернення: 13.02.2023).
20. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.
21. 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.

Інформаційні ресурси в Інтернеті

22. Веб-сайт URL: <https://uk.wikipedia.org/wiki/Веб-сайт> (дата звернення: 10.05.2023).
23. 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).
24. Відеохостинг URL: <https://uk.wikipedia.org/wiki/Відеохостинг> (дата звернення: 10.05.2023).
25. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.05.2023).
26. Інтернет-технології URL: <https://uk.wikipedia.org/wiki/Інтернет-технології> (дата звернення: 10.05.2023).
27. Криптовалюта URL: <https://uk.wikipedia.org/wiki/Криптовалюта> (дата звернення: 10.05.2023).
28. 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).
29. cyberpolice.gov.ua.
30. hackthebox.eu.
31. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.05.2023).
32. TRIM. URL: <https://ru.wikipedia.org/wiki/TRIM> (дата звернення: 10.05.2023).