МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Факультет № 4
Кафедра протидії кіберзлочинності

ЗАТВЕРДЖЕНО
На засіданні кафедри
протидії кіберзлочинності
протокол № 19 від 15.08.2023
Завідувач кафедри
Олександр МАНЖАЙ

Манжай Олександр Володимирович

ПРОТИДІЯ ТОРГІВЛІ ЛЮДЬМИ У КІБЕРСФЕРІ (ВК. 12)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Протидії кіберзлочинності (http://univd.edu.ua/uk/dir/1740/kafedra-informatsiynykh-tekhnologiy-ta-kiberbezpeky)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	moj@univd.edu.ua
Офіційна назва освітньої програми	Кібербезпека Cybersecurity
Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень та перший цикл

	вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	26 Цивільна безпека
Спеціальність	262 Правоохоронна діяльність
Спеціалізація	Поліцейські /підрозділи боротьби з торгівлею людьми/
Статус дисципліни	Вибіркова компонента освітньо-наукової програми, вивчається в 5 семестрі ІІІ курсу навчання
Мова викладання	Українська
Обсяг дисципліни в кредитах ECTS/годинах	4 кредити ECTS (загальний обсяг - 120 год.)
	аудиторна робота: 34 год. для денної форми навчання, з них:
	лекції: 10 год. для денної форми навчання
	семінарські заняття:
	практичні заняття: 34 год. для денної форми навчання
	самостійна робота: 76 год. для денної форми навчання
Час і місце проведення навчальної дисципліни	Аудиторія та час проведення заняття згідно розкладу
Консультації з навчальної дисципліни	Аудиторні консультації: аудиторія згідно графіку консультацій. Он-лайн-консультації: письмово в системі дистанційного навчання Moodle або електронною поштою викладача
Мета вивчення дисципліни	Навчити здобувачів вищої освіти особливостям використання комп'ютерних технологій працівниками поліції під час виявлення, попередження та розслідування кримінальних правопорушень. Виробити вміння щодо: застосовування норм законодавства у протидії кіберзлочинності; визначення методів протидії конкретним злочинам у сфері торгівлі людьми; застосування зарубіжного досвіду протидії злочинам у сфері торгівлі

	людьми з використанням комп'ютерних технологій; 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. 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.
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; моделі поліцейської розвідки; технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події; методи встановлення IP-адреси. 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. 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.
Форми та види проведення навчальних занять	Форма навчання – заочна. Види навчальних занять: лекції, семінарські, практичні, самостійна робота.
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
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.
Інтегральна компетентність, загальні компетентності, спеціальні (фахові) компетентності	Здатність і готовність особи розв'язувати завдання і проблеми у галузі правоохоронної діяльності, охорони прав і свобод людини, протидії злочинності, забезпечення публічної безпеки. ЗК.1 Здатність і готовність особи дотримуватися сукупності правових норм, які закріплюють і регулюють суспільні відносини, що забезпечують організаційну і функціональну єдність суспільства ЗК.4 Здатність до відповідальності за розвиток професійного знання і практик, оцінку стратегічного розвитку команди ЗК.5 Здатність і готовність особи

	створювати та оформлювати різні види документів у відповідності до правових, мовних та технічних норм документування та правил документообігу ФК.1 Здатність робити кваліфіковані юридичні висновки, давати консультації, застосовувати нормативно-правові акти в різних сферах юридичної та правоохоронної діяльності ФК.2 Здатність застосовувати законодавство України та спрямовувати свою діяльність у відповідності до вимог чинного законодавства (у тому числі антикорупційного) ФК.5 Здатність виявляти та аналізувати причини та умови, що сприяють вчиненню кримінальних та адміністративних правопорушень, вживати заходи для їх усунення ФК.6 Здатність систематизувати закономірності злочинності, визначати особу злочинця, причини і умови злочинності та її окремих видів, реалізовувати напрями і заходи її запобігання
ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ	
ТЕМА № 1 Засадничі принципи протидії злочинам у сфері торгівлі людьми Загальні питання використання інформаційних технологій під час торгівлі людьми. Загальні питання застосування інформаційних технологій правоохоронними органами для документування злочинів торгівлі людьми. Інформаційні технології, які використовуються для вербування жертв. Інформаційні технології, які використовуються для контролю та експлуатації жертв.	
ТЕМА № 2 Особливості використання технологій під час попередження та розслідування злочинів у сфері торгівлі людьми Інформаційні технології, які використовуються для комунікації, одержання коштів. Технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події. Аналіз даних великого об'єму. Методи і форми взаємодії правоохоронних органів у розслідуванні злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій.	
Результати навчання	ПРН 6. Розуміти принципи і мати навички

	етичної поведінки, соціально відповідальної та свідомої діяльності у сфері правоохоронної діяльності
	ПРН 10. Виокремлювати юридично значущі факти і формувати обгрунтовані правові висновки
	ПРН 15. Працювати автономно та в команді, виконуючи посадові обов'язки та під час розв'язання складних спеціалізованих задач правоохоронної діяльності
	ПРН 20. Підтримувати встанволені на законодавчому рівні умови дотимання дозвільної системи
Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль –залік, екзамен– 50 балів.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

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

Підсумкові бали навчальної дисципліни = Загальна кількість балів (перед підсумковим контролем) + Кількість балів за підсумковим контролем

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
90 – 100	Відмінно ("зараховано")	A	**„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.

80 – 89	Добре (“зараховано”)	B	**„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.
75 – 79		C	**„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.
68 –74	Задовільно (“зараховано”)	D	**„Задовільно”** – теоретичний зміст курсу освоєний не повністю, але прогалинине 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.
60 – 67		E	**„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.
35–59	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
1–34		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

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно-правові акти:

1. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.
2. 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.
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: 10.08.2021).
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. Про телекомунікації : закон України від 18.11.2003 : [із змінами і доповненнями]. *Офіційний вісник України*. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644.
6. 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.
7. Порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання : затверджений постановою Кабінету Міністрів України № 86 : від 28.01.2004 : [із

змінами і доповненнями] // Офіційний вісник України. 2004. № 4 (13.02.2004) (частина 1). Ст. 167.
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.
9. Online Investigative Principles for Federal Law Enforcement Agents. November 1999.
10. The Attorney General's Guidelines for Domestic FBI Operations. September 29, 2008.
11. The Attorney General's Guidelines On Federal Bureau Of Investigation Undercover Operations. May 30, 2002.
12. 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.
13. 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).
14. 互联网信息服务管理办法（国务院令第292号）. URL: http://www.gov.cn/gongbao/content/2000/content_60531.htm (дата звернення: 03.08.2021).

Основна література:

15. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності: монографія. Харків : Золота миля, 2012. 620 с.
16. 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.
17. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ*. 2016. № 3(74). С. 111-120.
18. 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.
19. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека*. 2009. № 4 (31). С. 215–219.
20. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.

Додаткова література:

21. Gibson W. Neuromancer. London: HarperCollins, 2010. 271 p.
22. Handbook of Digital Forensics and Investigation / edited by Eoghan Casey. Elsevier Academic Press, 2010. 567 p.

23. 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 c.
24. MD5. URL: https://ru.wikipedia.org/wiki/MD5 (дата звернення: 10.08.2021).
25. 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, 2010. NCJ 187736.
26. Practice Advice on Tackling Commercial Cannabis Cultivation and Head Shops. Bedfordshire: ACPO NPIA, 2010. 57 p.
27. Ribaux O. Reframing Forensic Science and Criminology for Catalyzing Innovation in Policing Practices. *Policing: A Journal of Policy and Practice*. 2019. Vol. 13, Iss. 1. pp. 5–11 (DOI: 10.1093/police/pax057).
28. 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. 2010. 41 p.
29. Дахно І. І. Зовнішньоекономічний менеджмент. К. : Центр учбової літератури, 2012. 568 с.
30. 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.
31. 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. 2010. С. 151-153.
32. 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.
33. 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.
34. 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.
35. Незаконні дії з банківськими платіжними картками: методичні

рекомендації. К. : МВС України, 2013. 28 с.
36. Панасюк І.В. Робота з великими текстовими масивами у правоохоронних органах // 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. 192–193.
37. 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.
38. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби // Теоретичні та прикладні питання економіки : збірник наукових праць. 2009. № 19. С. 338-342.
39. 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.

Інформаційні ресурси в Інтернеті

40. Case of Segerstedt-Wiberg and Others v. Sweden. URL: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-75591 (Дата звернення: 22.08.2021).
41. cyberpolice.gov.ua.
42. Comissioner's Operational Priorities. URL: https://www.police.gov.hk/ppp_en/01_about_us/cop.html(дата звернення: 31.07.2021).
43. Contents - EasyPatterns 2.5. URL: https://www.datamystic.com/textpipe/manual/general_usage_easypatterns_reference.htm (дата звернення: 09.08.2019).
44. 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: 03.08.2021).
45. hackthebox.eu.
46. 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: 10.08.2021).
47. Mission & Priorities. URL: https://www.fbi.gov/about/mission (дата звернення: 03.08.2021).
48. 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).
49. National Cyber Crime Unit. URL: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit (дата звернення: 10.082.2018).

50. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. URL: https://fr.wikipedia.org/wiki/Office_central_de_lutte_contre_la_criminalit%C3%A9_li%C3%A9e_aux_technologies_de_l%27information_et_de_la_communication (дата звернення: 03.08.2021).
51. Project 2020 Scenarios for the Future of Cybercrime – White Paper for Decision Makers. 25 p. URL: https://www.europol.europa.eu/sites/default/files/publications/2020_white_paper.pdf (дата звернення: 10.08.2021).
52. 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).
53. Schaar P. Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden. 5 p. URL: http://www.ccc.de/system/uploads/122/original/Schaar-Staatstrojaner.pdf/ (дата звернення: 03.08.2021).
54. Skype URL: https://uk.wikipedia.org/wiki/Skype (дата звернення: 10.07.2021).
55. Social bookmarking URL: http://en.wikipedia.org/wiki/Social_bookmarking (дата звернення: 10.07.2020).
56. TRIM. URL: https://ru.wikipedia.org/wiki/TRIM (дата звернення: 10.08.2021).
57. Viber URL: https://uk.wikipedia.org/wiki/Viber (дата звернення: 10.07.2021).
58. Веб-сайт URL: https://uk.wikipedia.org/wiki/Веб-сайт (дата звернення: 10.07.2021).
59. 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: 10.07.2021).
60. Відеохостинг URL: https://uk.wikipedia.org/wiki/Відеохостинг (дата звернення: 10.07.2021).
61. Електронна дошка оголошень URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень (дата звернення: 10.07.2021).
62. Інтернет-технології URL: https://uk.wikipedia.org/wiki/Інтернет-технології (дата звернення: 10.08.2021).
63. Кібербанди стають схожі на високоорганізовані синдикати. URL: http://unian.net/ukr/news/news-369195.html (дата звернення: 10.08.2021).
64. Криптовалюта URL: https://uk.wikipedia.org/wiki/Криптовалюта (дата звернення: 10.08.2021).