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

ЗАТВЕРДЖЕНО
На засіданні кафедри
протидії кіберзлочинності
протокол № 15 від 09 серпня 2022 р.
Завідувача кафедри
Олександр МАНЖАЙ

_____

Манжай Олександр Володимирович

Кримінальна розвідка у кіберсфері (ОК.06)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Протидії кіберзлочинності (https://univd.edu.ua/uk/dir/1740)
Розробник	Манжай Олександр Володимирович, завідувач кафедри протидії кіберзлочинності, кандидат юридичних наук, доцент
Контактний телефон	+38 057 7398085 (роб.)
E-mail	moj@univd.edu.ua
Навчальна дисципліна	Кримінальна розвідка у кіберсфері
Назва освітньо-професійної	Кібербезпека

програми	Cybersecurity
Рівень вищої освіти	Другий (магістерський) (НРК України – 7 рівень та другий цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технологій
Спеціальність	125 Кібербезпека
Спеціалізація	Безпека інформаційних та комунікаційних систем
Статус дисципліни	Обов'язкова компонента освітньо-наукової програми, вивчається в 1 семестрі І курсу навчання
Мова викладання	Українська
Обсяг дисципліни в кредитах ECTS/годинах	6 кредитів ECTS (загальний обсяг - 180 год.)
	аудиторна робота: 60 год. для денної форми навчання або 18 год. для заочної форми навчання, з них:
	лекції: 28 год. для денної форми навчання або 8 год. для заочної форми навчання
	практичні заняття: 16 год. для денної форми навчання або 6 год. для заочної форми навчання
	семінарські заняття: 16 год. для денної форми навчання або 4 год. для заочної форми навчання
	самостійна робота: 120 год. для денної форми навчання або 162 год. для заочної 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 з метою накопичення, обробки та аналізу інформації.

	Виробити вміння: застосовувати норми законодавства для здійснення аналітичної роботи; складати аналітичні висновки та представляти їх замовнику; застосовувати програмні засоби аналізу із графічним відображенням отриманих результатів; здійснювати віддалений збір інформації про вузли комп'ютерної мережі; шукати інформацію про об'єкти в мережі; здійснювати картографування злочинних проявів; оцінювати ступінь небезпечності об'єктів та суб'єктів кримінальної спрямованості. Сформувати у здобувачів вищої освіти знання, уміння і навички щодо порядку накопичення, обробки та аналізу інформації у кіберсфері; особливостей застосування різних програм для пошуку інформації у кіберсфері; моделей стримування злочинності; зарубіжного досвіду здійснення накопичення, обробки та аналізу інформації для вирішення завдань протидії кримінальним правопорушенням; географічного профілювання правопорушників; функціонування систем накопичення та обробки інформації.
Завдання вивчення дисципліни	Аналіз різних моделей стримування злочинності; дослідження поняття, завдання та функції кримінальної розвідки у кіберсфері; аналіз зарубіжного досвіду кримінальної розвідки у кіберсфері; вивчення особливостей здійснення розвідки з відкритих джерел; одержання навичок роботи з інструментами кримінальної розвідки.
Форми та види проведення навчальних занять	Форма навчання – денна або заочна. Види навчальних занять: лекції, практичні, семінарські, 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: екзамен.
Політика навчального курсу	Пропущені заняття відпрацьовуються усно за темою заняття згідно графіка консультацій викладача; перевірка тексту робіт на наявність текстових запозичень здійснюється програмою UNICHECK
Інтегральна компетентність, загальні компетентності, спеціальні (фахові) компетентності	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки ЗК.1 Здатність застосовувати знання у практичних ситуаціях ЗК.2 Здатність проводити дослідження на відповідному рівні ЗК.4 Здатність оцінювати та забезпечувати якість виконуваних робіт ФК.1 Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки ФК.6 Здатність аналізувати,

	контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації ФК.7 Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому
ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ	
ТЕМА № 1. Теоретичні засади розвідувально-аналітичної роботи Значення і місце розвідувально-аналітичної роботи в сучасних моделях стримування злочинності. Понятійний апарат розвідувально-аналітичної роботи правоохоронних органів. Організація здійснення розвідувально-аналітичної роботи.	
ТЕМА № 2. Методологія здійснення розвідувально-аналітичної роботи Етапи кримінальної розвідки. Загальні особливості аналітичної роботи. Особливості накопичення, обробки та аналізу даних великого об’єму.	
ТЕМА № 3. Окремі інструменти накопичення та аналізу розвідувальних відомостей Розвідка з відкритих джерел. Інструменти стратегічної кримінальної розвідки. Особливості накопичення та мережного аналізу електронних даних.	
ТЕМА № 4. Розвідувально-аналітична робота щодо груп злочинів Ідентифікація серійних правопорушень. Картографування злочинних проявів. Географічне профілювання.	

Результати навчання	ПРН 2 Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах ПРН 3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі ПРН 4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки ПРН 5 Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення ПРН 12 Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому ПРН 15 Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб ПРН 16 Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації,

	прогнозування та прийняття рішень ПРН 19 Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності ПРН 21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки ПРН 22 Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки
Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль –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**
97-100 **94-96** **90-93**	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.

85-89	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.
80-84			
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.
70-74	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.
65-69			
60-64		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.
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
21-40			

			можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
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
Орієнтовний перелік питань до заліку			1. Проактивні та реактивні системи стримування злочинності. 2. Визначення моделі поліцейської діяльності. 3. Науково-обґрунтована модель поліцейської діяльності (evidence-based policing). 4. Стандартна модель поліцейської діяльності (standard model of policing). 5. Модель поліцейської діяльності, орієнтована на потреби громади (community policing). 6. Модель нульової толерантності (zero tolerance policing). 7. Модель розбитих вікон (broken windows policing). 8. Облікова модель поліцейської діяльності (accountability model: CompStat, TrafficStat). 9. Проблемно-орієнтована модель поліцейської діяльності (problem-oriented policing). 10.Модель небезпечних зон (hot spots policing). 11.Модель поліцейської діяльності на основі розвідувальних відомостей (intelligence-led policing). 12.Прогностична модель поліцейської діяльності (predictive policing). 13.Історія розвитку розвідувально-аналітичної роботи поліції. 14.Співвідношення понять «розвідувально-

	аналітична робота», «кримінальна розвідка», «кримінальний аналіз». 15.Модель 3-і та її відмінність від моделі ILP. 16.Класифікація кримінальної розвідки за горизонтом реалізації. 17.Співвідношення понять «дані», «інформація», «знання», «розвідувальні відомості». 18.Співвідношення кримінальної розвідки та моделі ILP. 19.Кримінальна розвідка у кіберсфері. 20.Інтерпретація англомовної термінології у сфері розвідувально-аналітичної роботи. 21.Типові ролі суб'єктів, які залучаються до здійснення кримінальної розвідки. 22.Ресурсна база одержання розвідувальних відомостей. 23.Способи організації розвідувально-аналітичної роботи. 24.Особливості взаємодії аналітика з польовими працівниками. 25.Робоче місце аналітика. 26.Роль керівника розвідувально-аналітичного підрозділу. 27.Організація підготовки особового складу для роботи за проактивними моделями поліцейської діяльності. 28.Історія розробки та загальний зміст SOCTA. 29.Зміст поліцейського циклу. 30.Індикатори SOCTA та їх вага. 31.Проблемні питання впровадження сучасних підходів до розвідувально-аналітичної роботи. 32.Критерії ефективності модернізації розвідувально-аналітичної роботи. 33.Сенс кримінальної розвідки. 34.Стратегії кримінальної розвідки. 35.Види кримінальної розвідки. 36.Стратегічна кримінальна розвідка. 37.Інструменти і методи стратегічної кримінальної розвідки. 38.Тактична кримінальна розвідка. 39.Інструменти і методи тактичної

	кримінальної розвідки. 40.Оперативна кримінальна розвідка. 41.Інструменти і методи оперативної кримінальної розвідки. 42.Засоби кримінальної розвідки. 43.Застосування методології Anacapa у кримінальній розвідці. 44.Етапи кримінальної розвідки. 45.Постановка завдань як етап здійснення кримінальної розвідки. 46.Збирання даних як етап здійснення кримінальної розвідки. 47.Оцінка даних як етап здійснення кримінальної розвідки. 48.Системи оцінки 4x4, 5x5, 6x6. 49.Обробка даних як етап здійснення кримінальної розвідки. 50.Аналіз даних як етап здійснення кримінальної розвідки. 51.Дерево зв'язків (link charting). 52.Дерево подій (event charting). 53.Дерево цінностей (commodity flow charting). 54.Дерево дій (activity charting). 55.Фінансове профілювання (financial profiling). 56.Частотний графік (frequency charting). 57.Кореляція даних (data correlation) 58.Мережний аналіз даних. 59.Особливості побудови діаграм за даними про телефонні з'єднання. 60.Розробка аналітичних висновків як етап здійснення кримінальної розвідки. 61.Види аналітичних висновків. 62.Зміст аналітичних висновків. Система запитань 5W+H. 63.Етапи проведення аналізу конкуруючих гіпотез. 64.Поширення інформації як етап здійснення кримінальної розвідки. 65.Повторний аналіз інформації. 66.Джерела відкритої інформації. 67.Пошук інформації про об'єкти в мережі. 68.Збирання інформації про мережі даних. 69.Аналіз профілів соціальних мереж.

	70.Методи встановлення IP-адреси. 71.Аналіз заголовків електронних документів. 72.Аналіз метаданих. 73.Систематизація одержаної інформації. 74.Загальні інструменти для аналізу даних. 75.Використання MS Excel для вирішення завдань кримінальної розвідки. 76.Використання IBM i2 для вирішення завдань кримінальної розвідки. 77.Використання Maltego для вирішення завдань кримінальної розвідки. 78.Автоматизація групового накопичення та фіксації електронних даних, що становлять інтерес. 79.Збирання із наступним аналізом даних з месенджерів. 80.Накопичення та аналіз даних з сайтів з різноманітним контентом. 81.Завантаження та аналіз даних з соціальних мереж. 82.Автоматизація аналізу локальних таблиць з даними про рух фінансових цінностей. 83.Матричний аналіз як метод виявлення серійних правопорушень. 84.Контент-аналіз як метод виявлення серійних правопорушень. 85.Метод матричного аналізу IZE. 86.Сенс та завдання картографування злочинних проявів. 87.Створення простих точкових мап (pin mapping). 88.Картографування на основі ядерної оцінки густини (kernel density mapping). 89.Картографування з використанням пропорційних символів (proportional symbol mapping). 90.Застосування програмних інструментів картографування QGIS для вирішення завдань протидії кримінальним правопорушенням. 91.Використання інструментів картографування з метою прогнозування злочинності.

	92.Поняття та завдання географічного профілювання. 93.Теорії стандартної діяльності (routine activity), раціонального вибору (rational choice) та моделювання злочинів (crime pattern). 94.Типи просторової злочинної поведінки. 95.Прогнозування типу серійного злочинця. 96.Особливості методики профілювання М.Б. Ньютона. 97.Модель географічного таргетування злочинців (criminal geographic targeting) Д.К. Росмо. 98.Окремі математичні функції та методики для визначення місцезнаходження злочинця. 99.Програми географічного профілювання. 100. Відстані між помешканням злочинця та місцями вчинення злочинів.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно-правові акти:

1. Кримінальний процесуальний кодекс України : від 13.04.2012. *Голос України*. 2012. № 90-91.
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 елекронні комунікації : закон України від 16.12.2020 : [із змінами і доповненнями]. *Офіційний вісник України*. 2021. № 6 (26.01.2021). С. 10. Ст. 306.
4. 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.

Основна література:

5. Манжай О. В. Курс лекцій з дисципліни.
6. Criminal Intelligence. Manual for Analysts. United Nations, 2011. 96 p. – URL: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf (дата звернення: 17.05.2022).
7. Ratcliffe J. H. Intelligence-led Policing. 2nd edn. New York, NY: Routledge, 2016. 234 p.
8. Wang Liang & Zhao Jihong Solomon Contemporary police strategies of crime control in U.S. and China: a comparative study. *Crime, Law and Social Change*. 2016. № 5(66). pp. 525-537.
9. 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.
10. Потильчк А. О. Щодо співвідношення термінів «кримінальна розвідка» та «кримінальний аналіз» // *Прикарпатський юридичний вісник*. 2017. Вип. 1. Т. 5. С. 174-177.
11. Потильчак А. О. Що таке розвідувальні відомості в контексті моделі Intelligence-Led Policing? // *Visegrad journal on human rights*. 2019. № 6/3. с. 162-166.
12. Манжай О. В., Потильчак А. О. Особливості географічного профілювання у правоохоронних органах // *Право і безпека*. 2020. № 3(78). С. 13-21 (DOI: https://doi.org/10.32631/pb.2020.3.01).
13. Манжай О. В., Потильчак А. О. Особливості картографування злочинних проявів // *Право і безпека*. 2020. № 4(79). С. 66-72 (DOI: https://doi.org/10.32631/pb.2020.4.10).

Додаткова література:

14. Brown S. D. The meaning of criminal intelligence. *International Journal of Police Science & Management*. 2007. Vol. 9. No 4. pp. 336-340.
15. Guidance on the National Intelligence Model / Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence. 2005. 213 с. URL: https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf (дата звернення: 17.05.2022).
16. National Intelligence Model: Code of Practice. CENTREX, 2005. 14 p. URL: http://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf (дата звернення: 17.05.2022).
17. Ratcliffe J. H., Guidetti R. State police investigative structure and the adoption of intelligence-led policing. *Policing: An International Journal of Police Strategies & Management*. 2008. Vol. 31. Iss 1. P. 109-128 (DOI 10.1108/13639510810852602).
18. The National Criminal Intelligence Sharing Plan. Department of Justice. 2003. 54 p. URL: https://it.ojp.gov/documents/ncisp/National_Criminal_Intelligence_Sharing_Plan.pdf (дата звернення: 17.05.2022).
19. Манжай О. В., Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic National: Teorie si Practică*. 2015. № 3(13). С. 100-105.

Інформаційні ресурси в Інтернеті

20. inteltechniques.com