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

ЗАТВЕРДЖЕНО
На спільному засідання кафедри протидії кіберзлочинності факультету №4 та кафедри кібербезпеки та DATA-технологій факультету №6
протокол № 2 від 22.06.2023
Завідувач кафедри
Олександр МАНЖАЙ
_____

ЦИФРОВА КРИМІНАЛІСТИКА (ОК.22)

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)	
	**Носов Віталій Вікторович,** професор кафедри протидії кіберзлочинності факультету № 4, кандидат технічних наук, доцент E-mail: vitnos@univd.edu.ua **Лекційний потік:** факультет № 4, Ф4-402
Назва освітньо-професійної програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)
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
Спеціальність	125 Кібербезпека та захист інформації

Статус дисципліни	Нормативна компонента освітньо-наукової програми, вивчається в 7, 8 семестрах 4 курсу навчання
Мета вивчення дисципліни	формування знань і вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки
Завдання вивчення дисципліни	- отримання знань щодо криміналістичних досліджень сучасних інформаційних систем і носіїв даних; - формування вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки.
Обсяг дисципліни в кредитах ECTS/годинах	8 кредитів ECTS (загальний обсяг – 240 год.) З них (денна/заочна):
	- аудиторна робота: 120/24 год.
	- самостійна робота: 120/216 год.
Форми та види проведення навчальних занять	Форма навчання – денна/заочна Види навчальних занять: - лекції: 40/8 год.; - лабораторні заняття: 80/16 год.
Самостійна робота	Опрацювання рекомендованої літератури, виконання домашніх завдань до лабораторних занять, виконання індивідуальних завдань до лабораторних занять
Індивідуальні завдання	Наукові доповіді, індивідуальні завдання до лабораторних занять
Необхідне обладнання	Мультимедійне обладнання (ноутбук, проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	***Методи контролю***: поточний та підсумковий контроль (залік, екзамен) ***Форми контролю***: захист індивідуальних завдань на лабораторних заняттях, тестування, перевірка аудиторних контрольних робіт, перевірка виконання самостійних робіт, захист курсової роботи. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням.
Інтегральна компетентність, загальні компетентності (ЗК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

	ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.
Фахові компетентності (ФК)	ФК 1. Здатність застосовувати нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ

Тема № 1. Електронні (цифрові) докази

Цифрові дані як докази: визначення, роль, типи, характеристика, законодавчі вимоги. Характеристика криміналістичних досліджень. Типи кіберзлочинів, проблеми розслідувань, загальні правила криміналістичних досліджень. Типи електронних доказів. Криміналістичні дослідження як складова реагування на інциденти порушення кібербезпеки. Ролі та обов'язки осіб, що проводять криміналістичні дослідження. Загальна характеристика первинних цифрових криміналістичних досліджень.

Тема № 2. Процес первинних цифрових криміналістичних досліджень

Терміни та визначення понять. Загальний огляд процесу первинних цифрових криміналістичних досліджень. Ключові компоненти ідентифікації, збирання, здобуття та збереження цифрових доказів. Процес первинних цифрових криміналістичних досліджень: комп'ютерів, периферійних пристроїв та носіїв для зберігання цифрових даних, які не під'єднані до мережі; мережних пристроїв.

Тема № 3. Структура жорсткого диску та файлових систем

Типи жорстких дисків зберігання даних, їх характеристики. Фізична та логічна структура жорстких дисків. Розділи жорстких дисків. Завантаження з диску ОС Windows, Linux, Mac. Файлові системи ОС Windows, Linux, Mac. Відмінності різноманітних RAID систем зберігання. Порядок аналізу файлових систем.

Тема № 4. Здобуття даних та створення дублікатів носіїв даних

Загальний опис процесу здобуття даних. Здобуття даних наживо (live data). Здобуття сталих даних (static data). Послідовність у здобутті та дублюванні даних. Забезпечення незмінності оригінальних носіїв даних. Визначення ефективних методів і засобів здобуття даних. Здобуття даних з Windows і Linux комп'ютерів. Найкращі практики здобуття даних.

Тема № 5. Подолання протидії криміналістичним дослідженням

Поняття протидії криміналістичним дослідженням. Методи протидії криміналістичним дослідженням. Отримання доказів з видалених файлів і розділів, зашифрованих файлів, стеганографічних об'єктів. Ідентифікація обфускації, витирання залишків, перезапису даних та метаданих, шифрування.

Криптографічні мережні протоколи, програмні пакувальники, руткіти як методи протидії криміналістичним дослідженням. Контрзаходи протидії криміналістичним дослідженням. Основні виклики у подоланні протидії криміналістичним дослідженням.

Тема № 6. Криміналістичні дослідження операційних систем

Порядок здобуття і огляду стійких і нестійких даних з Windows комп'ютерів. Аналіз пам'яті і реєстру Windows. Огляд кешу, куків та історії веб-браузерів Windows.. Огляд файлів і метаданих в Windows. Аналіз журналів подій Windows. Аналіз журналів подій Linux. Здобуття і огляд стійких і нестійких даних з Linux комп'ютерів. Аналіз файлів і журналів подій Mac комп'ютерів.

Тема № 7. Криміналістичні дослідження комп'ютерних мереж

Сутність криміналістичного дослідження комп'ютерних мереж. Протоколювання трафіку комп'ютерної мережі. Принципи взаємозв'язків подій. Підготовка і етапи проведення криміналістичного дослідження комп'ютерних мереж. Огляд маршрутизатору, міжмережного екрану, системи виявлення вторгнень, DHCP-сервера, баз даних. Огляд трафіку. Документування отриманих із мережі доказів. Реконструкція доказів.

Тема № 8. Криміналістичні дослідження веб-атак

Сутність криміналістичного дослідження веб-атак. Архітектура веб-застосунків і виклики їх криміналістичного дослідження. Індикатори веб-атак і визначення загроз вебзастосункам. Етапи проведення криміналістичного дослідження веб-атак. Криміналістичне дослідження веб-атак на Windows сервери. Архітектура IIS веб-сервера і криміналістичний аналіз його лог-файлів. Архітектура Apache веб-сервера і криміналістичний аналіз його лог-файлів. Розслідування різноманітних атак на веб-застосунки.

Тема № 9. Криміналістичні дослідження баз даних

Сутність криміналістичного дослідження баз даних. Криміналістичне дослідження MS SQL. Виявлення репозитаріїв баз даних і збір файлів-доказів. Огляд файлів з використанням SQL Management Studio і ApexSQL DBA. Криміналістичне дослідження MySQL. Архітектура MySQL і визначення структури тек даних. Інструменти криміналістичного дослідження MySQL.

Тема № 10. Криміналістичні дослідження хмарних сервісів

Технології хмарних обчислень. Відомі атаки на технології хмарних обчислень. Сутність та завдання криміналістичного дослідження хмарних сервісів. Відмінності різних типів криміналістичного дослідження хмарних сервісів. Ролі зацікавлених сторін у криміналістичному дослідженні хмарних сервісів. Виклики, що виникають під час проведення криміналістичного дослідження хмарних сервісів. Криміналістичне дослідження хмарних сховищ Dropbox та Google Drive.

Тема- № 11.- Криміналістичні дослідження шкідливого програмного забезпечення

Шкідливе програмне забезпечення (ШПЗ) та шляхи його впровадження в систему. Методи розповсюдження ШПЗ. Основні складові ШПЗ. Принципи криміналістичного дослідження ШПЗ. Ідентифікація і вилучення ШПЗ з включеної і виключеної системи. Створення лабораторії і середовища з аналізу

шкідливих програм. Правила лабораторного аналізу ШПЗ. Динамічний і статичний аналіз. Виклики, що виникають під час проведення криміналістичного дослідження ШПЗ.	
Тема № 12. Криміналістичні дослідження електронної пошти Архітектура системи електронної пошти, сервери і клієнти, їх характеристики. Важливість електронних повідомлень. Злочини, де використовується електронна пошта. Складові листа електронної пошти, службові заголовки листа. Етапи криміналістичного дослідження електронних листів зловмисників і потерпілих. Інструменти криміналістичного дослідження електронної пошти.	
Тема № 13. Криміналістичні дослідження мобільних пристроїв Необхідність криміналістичного дослідження мобільних пристроїв. Роль апаратних і програмних платформ у криміналістичного дослідження мобільних пристроїв. Рівні архітектури оточення мобільних пристроїв. Стек архітектури Android і процеси завантаження системи. Стек архітектури iOS і процеси завантаження системи. Визначення місць збереження доказових даних. Підготовка до криміналістичного дослідження мобільних пристроїв. Криміналістичні дослідження мобільних пристроїв.	
Тема № 14. Складання звіту і представлення результатів криміналістичних досліджень Важливість оформлення звіту щодо результатів криміналістичних досліджень. Узагальнений шаблон звіту криміналістичних досліджень. Види звітів та методика їх складання. Спеціаліст з первинних криміналістичних досліджень як свідок. Порівняння ролей експертів і технічних спеціалістів. Свідчення спеціаліста у суді.	
Програмні результати навчання (ПРН)	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
	ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
	ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел щодо ефективного розв'язання спеціалізованих задач професійної діяльності.
	ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
	ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

	ПРН 6. Критично осмислювати основні теорії принципи, методи і поняття у навчанні та професійній діяльності.
	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 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
	ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
	ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.
	ПРН 55. Брати участь у попередженні, розкритті та розслідуванні правопорушень, здійснених з використанням можливостей кіберсфери
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 лабораторних заняттях (здобувач має отримати не менше 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: захист звітів лабораторних робіт 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	**Оцінка за**	**Оцінка за шкалою ECTS**

в балах	національною шкалою	Оцінка	Пояснення
97-100	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
94-96			
90-93			
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 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		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

<table>
<tr><td>40 – 59</td><td rowspan="2">Незадовільно («не зараховано»)</td><td>FX</td><td>«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</td></tr>
<tr><td>21 – 40</td><td></td></tr>
<tr><td>1–20</td><td>Незадовільно («не зараховано»)</td><td>F</td><td>«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</td></tr>
<tr><td colspan="4">Перелік питань, що виносяться на підсумковий контроль</td></tr>
<tr><td colspan="4">1. Поняття доказу і електронного доказу, законодавчі вимоги.
2. Особливості електронних (цифрових) доказів, рівні виявлення і фіксації цифрових слідів.
3. Типи кіберзлочинів, проблеми розслідувань, загальні принципи роботи з доказами із цифрових джерел інформації.
4. Ролі та обов’язки осіб, що проводять криміналістичні дослідження.
5. Основні та первинні цифрові криміналістичні дослідження, виконувачі первинних цифрових криміналістичних досліджень кримінального правопорушення.
6. Поняття ідентифікації, збирання, здобуття та зберігання цифрових доказів.
7. Поняття: копія цифрового доказу, функції верифікації, образ, виділений та невиділений простір.
8. Поняття: збереження, системний час, часовий штемпель, надійність.
9. Поняття: збіжність та відтворюваність, затвердження, псування та втручання.
10. Ролі, відповідальності, компетентності DEFR та DES.
11. Вирішення питання збирати чи здобувати потенційні цифрові докази.
12. Алгоритм збирання цифрових доказів - цифрові пристрої увімкнено.
13. Алгоритм збирання цифрових доказів - цифрові пристрої вимкнено.
14. Алгоритм здобуття цифрових доказів на увімкнених цифрових пристроях.
15. Алгоритм здобуття цифрових доказів на вимкнених цифрових пристроях.
16. Причини та процес часткового здобуття цифрових доказів.
17. Здобуття даних наживо (live data).
18. Здобуття сталих даних (static data).
19. Послідовність у криміналістичному дублюванні даних.
20. Визначення ефективних методів і засобів здобуття даних.</td></tr>
</table>

21. Методи протидії криміналістичним дослідженням.
22. Отримання доказів з видалених файлів і розділів, зашифрованих файлів, стеганографічних об’єктів.
23. Ідентифікація обфускації, витирання залишків, перезапису даних та метаданих, шифрування.
24. Криптографічні мережні протоколи, програмні пакувальники, руткіти як методи протидії криміналістичним дослідженням.
25. Контрзаходи протидії криміналістичним дослідженням.
26. Порядок здобуття і огляду стійких і нестійких даних з Windows комп’ютерів.
27. Аналіз пам’яті і реєстру Windows.
28. Огляд кешу, куків, історії веб-браузерів, файлів і метаданих в Windows.
29. Аналіз журналів подій Windows і Linux систем.
30. Здобуття і огляд стійких і нестійких даних з Linux комп’ютерів.
31. Сутність криміналістичного дослідження комп'ютерних мереж.
32. Протоколювання трафіку комп’ютерної мережі та принципи взаємозв’язків подій.
33. Підготовка і етапи проведення криміналістичного дослідження комп'ютерних мереж.
34. Криміналістичний огляд маршрутизатору, міжмережного екрану, системи виявлення вторгнень, DHCP-сервера, баз даних.
35. Криміналістичний аналіз трафіку.
36. Документування та реконструкція отриманих із мережі доказів.
37. Сутність криміналістичного дослідження вебатак.
38. Архітектура вебзастосунків і виклики їх криміналістичного дослідження.
39. Індикатори вебатак і визначення загроз вебзастосункам.
40. Етапи проведення криміналістичного дослідження вебатак.
41. Криміналістичне дослідження вебатак на Windows сервери.
42. Архітектура IIS вебсервера і криміналістичний аналіз його логфайлів.
43. Архітектура Apache вебсервера і криміналістичний аналіз його логфайлів.
44. Розслідування різноманітних атак на вебзастосунки.
45. Сутність криміналістичного дослідження баз даних.
46. Криміналістичне дослідження MS SQL.
47. Виявлення репозиторіїв баз даних і збір файлів-доказів.
48. Огляд файлів з використанням SQL Management Studio і ApexSQL DBA.
49. Криміналістичне дослідження MySQL.
50. Архітектура MySQL і визначення структури тек даних. I
51. Криміналістичне дослідження MySQL на WordPress.
52. Сутність та завдання криміналістичного дослідження хмарних сервісів.
53. Відмінності різних типів криміналістичного дослідження хмарних сервісів.
54. Ролі зацікавлених сторін у криміналістичному дослідженні хмарних сервісів.
55. Виклики, що виникають під час проведення криміналістичного дослідження хмарних сервісів.
56. Криміналістичне дослідження хмарних сховищ Dropbox та Google Drive.
57. Принципи криміналістичного дослідження ШПЗ.
58. Ідентифікація і вилучення ШПЗ з включеної і виключеної системи.

59. Створення лабораторії і середовища з аналізу шкідливих програм.
60. Правила лабораторного аналізу ШПЗ. Динамічний і статичний аналіз.
61. Виклики, що виникають під час проведення криміналістичного дослідження ШПЗ.
62. Етапи криміналістичного дослідження електронних листів зловмисників і потерпілих.
63. Підготовка до криміналістичного дослідження мобільних пристроїв.
64. Криміналістичні дослідження мобільних пристроїв.
65. Узагальнений шаблон звіту криміналістичних досліджень. Види звітів та методика їх складання.
66. Спеціаліст з первинних криміналістичних досліджень як свідок.
67. Порівняння ролей експертів і технічних спеціалістів. Свідчення спеціаліста у суді.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. EC-Council. Computer Hacking Forensic Investigator v9. Courseware.
2. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів.
3. Стандартні робочі процедури для збирання, аналізу та демонстрації електронних доказів / Офіс програми протидії кіберзлочинності Ради Європи (C-PROC) / Електронна версія від 12 вересня 2019 року.
4. Посібник з питань електронних доказів. Базовий посібник для співробітників правоохоронних органів, прокурорів та суддів / Відділ протидії кіберзлочинності. Генеральний директорат з прав людини та верховенства права Ради Європи / Електронна версія 2.1, Страсбург, Франція, 6 березня 2020 року.
5. 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.
6. Посібник для підвищення кваліфікації працівників органів та підрозділів Національної поліції України / О.І. Безпалова, КЛ. Бугайчук, А.В. Волховський та ін. Харків, нац. ун-т внутр. справ. Харків: ХНУВС. 2019. 132 с.

ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Third Edition. Edited by Eoghan Casey. www.elsevierdirect.com/companions/9780123742681.
2. Handbook of Digital Forensics and Investigation Edited by Eoghan Casey. http://www.elsevierdirect.com/product.jsp?isbn=9780123742674.
3. Digital Forensics and Preservation. Digital Preservation Coalition and Jeremy

Leighton John. [Електронний ресурс] / Published in association with Charles Beagrie Ltd. 2012. Режим доступу: http://dx.doi.org/10.7207/twr12-03.

Інформаційні ресурси в Інтернеті:

1. https://securityonline.info/category/forensics/
2. https://resources.infosecinstitute.com/category/forensics-2/
3. http://www.dfrws.org/
4. https://www.forensicmethods.com