ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 08 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Цифрова криміналістика
Назва дисципліни

Призначення Робочої програми	Для освітніх програм різних спеціальностей
Рівень вищої освіти*	Другий (магістерський)
Мова навчання	Українська
Обсяг дисципліни, кредитів ЄКТС	8
Статус дисципліни	Вибіркова
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма здобуття освіти	Обсяг дисципліни		Кількість годин						Форма семестрового контролю
			Аудиторні заняття					Самостійна робота (в т.ч. ІРС)	
	Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття		Залік
Д	8	240	66	32	34			174	+

Примітка: *Вибіркову навчальну дисципліну, яку кафедра рекомендує для певного рівня вищої освіти / спеціальності, мають право вибирати здобувачі інших рівнів та спеціальностей університету.

Робоча програма складена _____ канд. техн. наук, доц. Віктор ЧЕШУН
Підпис Науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Схвалена на засіданні кафедри кібербезпеки

Протокол від « 29 » 08.2025 р. №1

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

2. Пояснювальна записка

Дисципліна «Цифрова криміналістика» відноситься до циклу вибіркових дисциплін та охоплює сучасні підходи до розкриття та інтерпретації електронних даних в процесі накопичення цифрових доказів, а також до збереження будь-яких доказів у їхньому первісному вигляді під час проведення структурованого розслідування шляхом збору, ідентифікації та перевірки цифрової інформації з метою реконструкції минулих подій.

Мета дисципліни. Формування у здобувачів вищої освіти теоретичних знань і практичних навичок щодо вирішення типових та складних завдань цифрової криміналістики, що полягають у зборі цифрової криміналістичної інформації, збереженні, дослідженні і використанні цифрових доказів.

Предмет дисципліни. Основні поняття, методи та засоби цифрової криміналістики.

Завдання дисципліни. Формування практичних навичок застосування методів і засобів збору криміналістичної інформації з комп'ютерних систем і носіїв даних, а також розпізнавання та документування електронних доказів з метою їх використання у розслідуваннях та суді.

Результати навчання. Після вивчення дисципліни студент повинен: *знати* теоретичні основи і сучасні інформаційні технології аналізу та збору цифрової криміналістичної інформації; *вміти* застосовувати методи цифрової криміналістики; досліджувати дані і визначити джерела даних; *вміти* отримувати і описувати цифрові докази; застосовувати способи аутентифікації цифрових доказів; *вміти* порівнювати і зіставити цифрові докази і традиційні докази для встановлення відмінностей між ними; *використовувати і критично аналізувати* моделі процесів цифрової криміналістики; *застосовувати* національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів; *застосовувати* стандарти і передові практичні методи, що стосуються цифрових доказів в цифровій криміналістиці; *володіти* основними поняттями, методами та інструментами цифрової криміналістики; володіти навичками збору і аналізу цифрової криміналістичної інформації, способами аутентифікації цифрових доказів; *володіти* умінням самостійно опановувати нові методи та технології розслідування кіберзлочинів та запобігання кіберзлочинам.

3. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:		
	лекції	**лабораторні**	**СРС**
Тема 1. Вступ до науки цифрової криміналістики (DFS)	4	4	21
Тема 2. Основи комп'ютерної грамотності фахівця з DFC	4	4	21
Тема 3. Докази цифрової криміналістики	2	4	11
Тема 4. Місце злочину	8	8	42
Тема 5. Розділи цифрової криміналістики	8	8	42
Тема 6. Антикриміналістика	4	6	21
Тема 7. Експертиза й аналіз	2	-	16
Разом за семестр:	**32**	**34**	**174**

4. Програма навчальної дисципліни

4.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Тема 1. Вступ до науки цифрової криміналістики (DFS)	***4***
1	**Введення в цифрову криміналістику.** Вступ до цифрової криміналістики. Визначення цифрової криміналістики.	2

	Наука цифрової криміналістики. Спільноти у сфері цифрової криміналістики. Цифрова криміналістика, Кіберкриміналістика чи Комп'ютерна криміналістика? Визначення цифрової криміналістики – паразитуючі міфи і вплив медіа. Літ.: [1] с.7-17; [2] с.14-46; [3] с.46-50; [8] с.8-66	
2	**Основні поняття і визначення цифрової криміналістики.** Контекст цифрової криміналістики. Заходи кіберкриміналістики. Цифрова криміналістика в різних контекстах. Науковий підхід в цифровій криміналістиці. 1. Підсумок за темою 1 Літ.: [1] с.7-17; [2] с.47-87; [8] с.67-86	2
	Тема 2. Основи комп'ютерної грамотності фахівця з DFC	***4***
3	**Жорсткі диски – фізична і логічна організація** Основи комп'ютерної грамотності – цілі навчання. Основні типи дисків. Жорсткий диск (HDD) порівняно із твердотілим накопичувачем (SSD). Структури жорсткого диска (HDD). Розрахунок ємності накопичувача. Адресація жорсткого диска. Розбиття або поділ диска на розділи і типи форматів. Головна таблиця розділів. Коди типів розділу, hex-коди типів розділу. Варіанти розбиття (поділу) диска. Приховані розділи. Область, захищена хостом (HPA). Оверлей конфігурації диска (DCO). Літ.: [4] с.19-20	2
4	**Процес завантаження** Процес завантаження – основні поняття. Процес завантаження – формат для старіших версій (Legacy). Процес завантаження – UEFI. Процес завантаження – Windows UEFI. Процес завантаження – POST. Процес завантаження Windows 10. Процес завантаження Linux. Процес завантаження Unix. Процес завантаження Mac OS 11. Літ.: [4] с.20-22	2
	Тема 3 – Докази цифрової криміналістики	***2***
5	**Розташування та види доказів** Види цифрових доказів. Розташування доказів. Розташування доказів – електронна пошта. Розташування доказів – принтери. Розташування доказів – пристрої Roku, медіаплеєри Fire Sticks. Розташування доказів – маршрутизатори (роутери). Розташування доказів – Raspberry Pi (одноплатні комп'ютери). Геолокація. Фото і відео. EXIF (Exchangeable Image File Format – придатний до обміну формат файлів зображень) [Метадані]. Місцеположення iPhone. Геолокація IP. Місця розташування за соціальними мережами. Теги геолокації за соціальними мережами. Розташування стільникових веж. Літ.: [1] с.24-30; [2] с.122-139	2
	Тема 4. Місце злочину	***8***
6	**Принцип обміну та збір доказів на місці злочину** Принцип обміну. Що таке місце злочину? Докази на місці злочину. Принципи криміналістики. Виявлення цифрових (електронних) доказів. Процедури, яких слід дотримуватися на місці злочину. Контрольний список, обґрунтований з погляду криміналістики. Набори для роботи експерта-криміналіста на виїзді. Літ.: [1] с.31-40; [2] с.140-198; [4] с.69-80; [7] с.112-117	2
7	**Цифрові (електронні) докази** Цифрові (електронні) докази. Вилучення та збереження доказів. Докази на комп'ютері. Докази на телефоні. Докази у хмарних сховищах. Докази в	2

	мережі. Середовище, що стосується розслідування (ІЕ). ІЕ – техніки. ІЕ – міркування Дауберта. ІЕ – інструменти. ІЕ – технології. ІЕ – автоматизація. ІЕ – планування Літ.: [1] с.18-23; [2] с.122-139; [4] с.31-42; [7] с.117-120	
8	**Інструменти цифрової криміналістики** Стислий огляд інструментів цифрової криміналістики. Апаратні блокувальники запису. Програмні блокувальники запису. Чому використовуються образи/зображення. Побітова копія (копія бітового потоку) порівняно з резервною копією. Криміналістичний образ (зображення): Фізичний диск. Криміналістичний образ (зображення) логічного тому. Хеш-функція MD5 для цілісності образу (зображення) даних. Огляд програмного забезпечення для створення образів. Програмне забезпечення для створення образів – FTK Imager. Мобільні системи для роботи експерта-криміналіста на виїзді (MFS). Вимоги до інструментів для створення образів дисків. Набори для роботи експерта-криміналіста на виїзді Літ.: [3] с.58-62; [7] с.13-45	2
9	**Проведення досліджень** Криміналістичне мислення. Хронологія подій у рамках розслідування. MAC times (частини метаданих файлової системи). Організація проведення розслідування. Запитання в рамках розслідування. Модель проведення експертизи доказів у цифровій криміналістиці. Запитання в рамках розслідування – Заитання/Запити. Реєстр Windows. HKEY_CLASSES_ROOT. Інструменти реєстру. Файли ntuser.dat та index.dat. Інструменти управління провадженнями. Літ.: [1] с.42-58; [4] с.24-30, 135-160; [7] с.111-112, 121-124	2
	Тема 5. Розділи цифрової криміналістики	***8***
10	**Криміналістика хостів** Криміналістика хостів – об'єкти. Криміналістика хостів. Криміналістика хостів – віртуальні машини. Літ.: [4] с. 105-112; [5] с. 8-81; [6] с. 1-37	2
11	**Криміналістика електронної пошти і миттєвих повідомлень** Криміналістика електронної пошти і миттєвих повідомлень – введення. Криміналістика електронної пошти і миттєвих повідомлень. Розслідування електронної пошти Літ.: [4] с. 227-240; [5] с. 184-207; [6] с. 68-81	2
12	**Мережева криміналістика** Що таке мережева криміналістика? Основи криміналістичного аналізу мережі. Атаки мережі. Які докази можна зібрати? Інструменти мережевої криміналістики. Що слід запам'ятати для успіху мережевої криміналістики. Літ.: [4] с. 113-117; [6] с. 38-46	2
13	**Криміналістика мобільних пристроїв** Криміналістика мобільних пристроїв – введення. Криміналістика мобільних пристроїв і Геді Ламар. Перелаштування частоти. CDMA. Мобільні телефони в історії. Що нас цікавить? Види доказів. Криміналістика мобільних пристроїв та вбудованих систем як наука. Синергія Літ.: [4] с. 252-255; [5] с. 208-275; [6] с. 46-54	2
	Тема 6. Антикриміналістика	***4***
14	**Антикриміналістика в розрізі технік і операційних систем** Поширені техніки. Антикриміналістика. Область свопінгу. Антикриміналістика Windows. Антикриміналістика FS Unix. Зарезервований простір. Альтернативні потоки даних (ADS). Підсумки щодо приховання даних. Літ.: [5] с. 59-81	2

15	**Антикриміналістика файлових структур. Стеганографія і стеганоаналіз** Видалення, переформатування та сміттєвий кошик. Зберігання файлів у NTFS. Видалені файли. Видалення файлу. Надсилання в кошик / видалення каталогу. Видалені файли у NTFS. Заповнювачі. Файл INFO2. Desktop.ini. Стеганографія. Стеганоаналіз. Інструменти для виявлення слідів стеганографії. Літ.: [5] с. 114-131	2
	Тема 7. Експертиза й аналіз	***2***
16	**Експертиза й аналіз** Моделі розслідування. ADFM. IDIP. EIDIP. HOBFDIP. Критика моделей. Аналіз цифрового місця злочину. Якісна криміналістична процедура. Аналіз категорій. Вимоги до аналітичних інструментів. Атрибуція – поняття і фази. Підходи Ческі. Сценарії атрибуції. Виклики атрибуції. Підсумок лекції. Літ.: [3] с.51-57; [6] с. 82-114; [7] с.125-128; [9] с.24-34	2
	Разом:	**32**

4.2 Зміст лабораторних занять

№ з/п	Тема лабораторного заняття	Кількість годин
	Тема 1. Вступ до науки цифрової криміналістики (DFS)	***4***
1	Збір та аналіз цифрової криміналістичної інформації засобами операційної системи Літ.: [4] с. 135-145, 148-160; [5] с. 8-81; [6] с. 1-37	4
	Тема 2. Основи комп'ютерної грамотності фахівця з DFC	***4***
2	Відновлення прихованої та знищеної цифрової криміналістічної інформації на накопичувачах різних видів. Літ.: [4] с. 146-147; [5] с. 82-113	4
	Тема 3 – Докази цифрової криміналістики	***4***
3	Отримання цифрової криміналістічної інформації, заблокованої парольною аутентифікацією. Літ.: [4] с.43-56	4
	Тема 4. Місце злочину	***8***
4	Збір та аналіз цифрової криміналістичної інформації програмою для електронної експертизи FTK. Літ.: [4] с. 205-219; [6] с. 38-46	4
5	Збір та аналіз цифрової криміналістичної інформації з носіїв даних програмою Autopsy. Літ.: [4] с. 179-191	4
	Тема 5. Розділи цифрової криміналістики	***8***
6	Збір та аналіз цифрової криміналістичної інформації в мережі Internet. Літ.: [4] с. 227-240; [6] с. 55-81	4
7	Збір та аналіз цифрової криміналістичної інформації з мобільних пристроїв засобами Wondershare Dr.Fone for Android Літ.: [4] с. 252-255; [5] с. 208-275; [6] с. 46-54	4
	Тема 6. Антикриміналістика	***6***
8	Антикриміналістика інструментами стеганографії Літ.: [5] с. 114-131	4
9	Узагальнення матеріалу. Тестування.	2
	Разом:	**34**

4.3 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до лабораторних

занять, тестування тощо. Керівництво самостійною роботою здійснюється викладачем згідно з розкладом консультацій у позаурочний час. Крім цього до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

Номер тижня	**Вид самостійної роботи**	**Кількість годин**
1-2	Опрацювання теоретичного матеріалу. Підготовка до ЛР1. Підготовка до захисту ЛР1.	21
3-4	Опрацювання теоретичного матеріалу. Підготовка до ЛР2. Підготовка до захисту ЛР2.	21
5-6	Опрацювання теоретичного матеріалу. Підготовка до ЛР3. Підготовка до захисту ЛР3	21
7-8	Опрацювання теоретичного матеріалу. Підготовка до ЛР4. Підготовка до захисту ЛР4.	21
9-10	Опрацювання теоретичного матеріалу. Підготовка до ЛР5. Підготовка до захисту ЛР5	21
11-12	Опрацювання теоретичного матеріалу. Підготовка до ЛР6. Підготовка до захисту ЛР6.	21
13-14	Опрацювання теоретичного матеріалу. Підготовка до ЛР7. Підготовка до захисту ЛР7.	21
15-16	Опрацювання теоретичного матеріалу. Підготовка до ЛР8. Підготовка до захисту ЛР8	21
17	Опрацювання теоретичного матеріалу. Підготовка до тестування.	6
	Разом за семестр:	**174**

***Примітки*:** ЛР – лабораторна робота

5. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: лекції (з використанням словесних та наочних методів, мультимедійних технологій, проблемного й інтерактивного навчання, мотиваційних прийомів); лабораторні заняття (з використанням частково-пошукових і контекстних методів, аналізу проблемних ситуацій, розвитку критичного мислення, пояснення, елементів дискусії тощо); самостійна робота (опрацювання програмного матеріалу з відповідних джерел інформації, підготовка до виконання і захисту лабораторних робіт, тестування тощо), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

6. Методи контролю

Поточний контроль здійснюється під час аудиторних лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

– оцінювання результатів захисту лабораторних робіт;

– тестовий контроль засвоєння теоретичного та практичного матеріалу.

Підсумкова семестрова оцінка виставляється за результатами поточного контролю. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

7. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-

методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття (наведені у Методичних рекомендаціях до лабораторних занять)), активно працювати на занятті, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами лабораторних робіт тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час лабораторних занять, тестування.

Здобувач вищої освіти, виконуючи лабораторні роботи та тестування з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах, які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

8. Оцінювання результатів навчання студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**

Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів денної форми здобуття освіти у семестрі

Аудиторна робота								**Контрольні заходи**	**Семестровий контроль**
Лабораторні заняття №:								Тестовий контроль	Залік
1*	2	3	4	5	6	7	8	Т 1-7	
Кількість балів за кожний вид навчальної роботи (мінімум-максимум)									
6-10	6-10	6-10	6-10	6-10	6-10	6-10	6-10	12-20	За рейтингом
48-80								**12-20**	**60-100****

Примітки: Т – тема навчальної дисципліни;

*За набрану з будь-якого виду роботи (дисципліни) кількість балів нижче встановленого мінімуму здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; знання застосовуваних методів і засобів цифрової криміналістики, повнота відповіді на контрольні питання тощо.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів навчання з теоретичного матеріалу

Тест, передбачений Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	0-59	60-65		66-72	73-82		83-89	90-100		
Кількість балів	-	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий залік виставляється на останньому занятті за умови, що загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна оцінка** (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)	
		Залік	**Іспит/диференційований залік**
A	90-100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		
D	66-72		***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для

E	60-65		подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
FX	40-59	Незараховано	***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

9. Питання для самоконтролю результатів навчання

1. Передумови виникнення цифрової криміналістики. Сфери застосування цифрової криміналістики.
2. Основні задачі цифрової криміналістики.
3. Спільноти цифрової криміналістики.
4. Цифрова криміналістика, Кіберкриміналістика і Комп’ютерна криміналістика – порівняльний аналіз.
5. «Три А» цифрової криміналістики.
6. Принцип обміну Локара.
7. Заходи кіберкриміналістики.
8. Цифрова криміналістика в різних контекстах.
9. Форензика – прикладна наука про розкриття злочинів пов'язаних з комп'ютерною інформацією.
10. Поняття комп'ютерний злочин.
11. Криміналістична характеристика. Статистика. Особистість ймовірного злочинця. Оперативність.
12. Типові комп’ютерні злочини та дія криміналіста: ідентифікація способу створення, злочинця, слідів, постраждалого.
13. Шахрайство із трафіком: ідентифікація способу створення, злочинця, слідів, постраждалого.
14. Порушення авторських прав у офлайні: ідентифікація способу створення, злочинця, слідів, постраждалого.
15. Порушення авторських прав у Мережі: ідентифікація способу створення, злочинця, слідів, постраждалого.
16. Фішинг: ідентифікація способу створення, злочинця, слідів, постраждалого.
17. Кіберсквотинг: ідентифікація способу створення, злочинця, слідів, постраждалого.
18. Платежі через Інтернет: ідентифікація способу створення, злочинця, слідів, постраждалого.
19. Шахрайство в онлайнових іграх: ідентифікація способу створення, злочинця, слідів, постраждалого.
20. Використання RBL: ідентифікація способу створення, злочинця, слідів, постраждалого.
21. Накрутка: ідентифікація способу створення, злочинця, слідів, постраждалого.
22. Правова оцінка злочинів.
23. Правила поводження із доказами (управління доказами) в реагуванні на інциденти.
24. Етап підготовки в реагуванні на інциденти.
25. Процедури виявлення і аналізу в реагуванні на інциденти.
26. Стримування в реагуванні на інциденти.
27. Ліквідація наслідків в реагуванні на інциденти. Відновлення.
28. Діяльність після кіберінцеденту.
29. Виявлення проблемних аспектів цифрової криміналістики.
30. Технічні проблеми цифрової криміналістики.
31. Правові аспекти і проблеми цифрової криміналістики.
32. Проблеми криміналістики мобільних технологій. Проблеми криміналістики в мережевих системах.
33. Аналіз принципів будови сучасних комп’ютерів як об’єкта цифрової криміналістики.
34. Носії інформації – фізична і логічна будова.

35. Основні методи приховування цифрових доказів.
36. Пошук і відновлення цифрових доказів.
37. Види цифрових доказів.
38. Методи пошуку цифрових доказів.
39. Отримання та закріплення цифрових доказів.
40. Процеси і сервіси операційних систем. Засоби операційних систем як інструменти цифрової криміналістики.
41. Перехоплення та дослідження трафіку. Шифрований трафік. Дослідження статистики трафіку. Netflow.
42. Модель Крузе і Хайзера.
43. Модель Міністерства юстиції США (USDOJ).
44. Модель DFRWS.
45. Абстрактна цифрова криміналістична модель.
46. Інтегрований процес цифрового розслідування (IDIP).
47. Модель розширеного процесу цифрового розслідування (EDIP).
48. Модель процесу польового сортування комп'ютерної криміналістичної експертизи (CFFTPM).
49. Загальна модель процесу розслідування комп’ютерної криміналістичної експертизи (GCFIPM).
50. Класифікація, принципи дії і призначення засобів розслідування цифрових інцидентів і захисту інформації.
51. Блокатори запису.
52. Устаткування для знімання даних.
53. Проблеми зберігання, передачі та обробки цифрових доказів у комп'ютерній криміналістиці.
54. Принципи і способи запобігання витоку інформації. Засоби запобігання витоку інформації: пристрої знищення даних, інформаційні сейфи тощо.
55. Методи стеганографії і приховування цифрових доказів. Приховування даних у текстових файлах.
56. Приховування даних у нерухомих зображеннях.
57. Приховування даних у просторовій області і у частотній множині зображень.
58. Приховування даних в звукових та відео файлах.

10. Навчально-методичне забезпечення

Освітній процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі для навчання: https://msn.khmnu.edu.ua/course/view.php?id=8033.

11. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп’ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, мультимедійний проєктор. Програмне забезпечення: програми Microsoft Office або аналогічні, доступ до мережі Інтернет, робота з презентаціями.

Матеріально-технічне забезпечення лабораторного практикуму: ПК або ноутбук, смартфон.

Програмне забезпечення лабораторного практикуму: операційна система (Windows або Linux тощо), Accent RAR Password Recovery (демо версія), R-Studio (shareware), UFS Explorer Standard Recovery (shareware), AD Forensic Tool Kit (trial), Autopsy (open source digital forensics platform), Dr. Fone-Data Recovery (демо версія), OpenStego (free and open source steganography software).

12. Рекомендована література:

Основна

1. Вступ до цифрової криміналістики : навч. посіб. / В. Ю. Шепітько та ін. ; за ред. В. Ю. Шепітька. Харків : Право, 2025. 124 с. URL: https://shorturl.at/1lKAC

2. Кіберзлочинність та електронні докази : навч. посібник / Б. М. Головкін та ін. ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

3. Степанюк Р. Л., Гусєва В. 0. Сучасні криміналістичні засоби та методи протидії злочинності: навч. посіб. Харків : ХНУВС, 2024. 232 с. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi78/0058151.pdf

4. Joakim Kavrestad, Marcus Birath, Nathan Clarke. Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications. Third Edition. Springer, 2024. 297 p. URL: https://books.google.com.ua/books?id=V6f8EAAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

5. Suhas Pednekar, Ravindra D. Kulkarni, Prakash Mahanwar. Cyber forensics. Published by Director Institute of Distance and Open Learning, University of Mumbai, Vidyanagari, Mumbai - 400 098, 2022. 275 p. URL: https://mu.ac.in/wp-content/uploads/2022/06/M.Sc.IT-Paert-II-CBCS-Cyber-Forensicssemester-IV-2.pdf

6. Shirke D. T., Ajay Bhamare, Prakash Mahanwar. TYBSC CS Cyber Forensics. Published by Director Institute of Distance and Open Learning, University of Mumbai, Vidyanagari, Mumbai - 400 098, 2023. 147 p. URL: https://www.scribd.com/document/808269214/TYBSC-CS-Cyber-forensics

7. Криміналістика: криміналістична техніка : навчальний посібник / Р. Л. Степанюк та ін. Харків : ХНУВС, 2023. 388 с. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi75/0055786.pdf

8. Криміналістика : підручник / Р. І. Благута та ін. ; за заг. ред. Є. В. Пряхіна. 4-те вид., перероб. і допов. Львів : Львівський державний університет внутрішніх справ, 2023. 820 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/7336/1/криміналістика_макет_print.pdf

9. Тіщенко В. В., Подобний О. О. Криміналістика : навчально-методичний посібник. Одеса : Видавництво «Юридика», 2022. 236 с. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/27d635b0-3ef7-4509-8680-12739ea5a8e9/content

10. Digital Notes on 410244(C): Cyber Security and Digital Forensics. SAK, Department of Computer ENGG. 2022-23. 261 p. URL: https://erp.metbhujbalknowledgecity.ac.in/StudyMaterial/01SK102021010300023.pdf

11. Tech B. Digital Notes On Digital Forensics. Malla Reddy College of Engineering & Technology ; Autonomous Institution – UGC, Govt. of India 2022. 136 p. URL: https://mrcet.com/downloads/digital_notes/CSE/III%20Year/12082022/DIGITAL%20FORENSICS.pdf

12. Кушнір М. Я., Цеханський В. Д. Законодавчі питання інформаційної безпеки: Електронний навчальний посібник. Чернівці : Чернівецький національний університет, 2024. 102 с. URL: https://drive.google.com/file/d/1r7JUzLpdq-RM2Oq-iDM_Uzk3nG4V2wAC/view

13. Правове регулювання національної безпеки : навчальний посібник / О. Г. Боднарчук та ін. Ірпінь: Державний податковий університет, 2024. 202 с. URL: https://dpu.edu.ua/images/Documents/NAUKA/Naukova%20biblioteka/Navcalno-metodicna%20literatura/N/Pravove%20reguluvanna%20nacionalnoi%20bezpeki.pdf

14. Кримінально-правова охорона інформаційної безпеки в Україні: монографія / В. І. Борисов та ін.; за заг. ред. В. І. Борисова, О. О. Пащенка ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 328 с. DOI: https://doi.org/10.31359/9786178518899.

Додаткова

15. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : редакція від 09.08.2024. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 28.08.2025).

16. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://izmail.maup.com.ua/biblioteka/akademichna-dobrochesnist2/dstu-8302-2015/prikladi-oformlennya-bibliografichnih-posilan-dstu-8302-2015 (дата звернення: 28.08.2025).

17. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата

звернення: 28.08.2025).

18. Цифрова криміналістика : консп. лекцій / уклад. І. З. Якименко. Тернопіль : ТНЕУ, 2019. 109 с.

19. Digital Forensics / Edited by André Årnes. – John Wiley & Sons Ltd, 2018. 336 p.

20. Cybercrime: University Module Series, Teaching Guide. / United Nations Office on Drugs and Crime. Vienna, United Nations, Doha Declaration, 2019. 453 p.

21. Digital Forensics Basics: A Practical Guide Using Windows OS/ Edited by Nihad A. Hassan. New York, 2019. 335 p.

22. Конахович Г. Ф. , Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. Київ: «Центр учбової літератури», 2018. 558 с

23. Bashar ALEsawi. Introduction To Digital Forensics. Mustansiriyah University, College of Science - Department of CS/Cybersecurity, 2024. 28 p. URL: https://uomustansiriyah.edu.iq/media/lectures/6/6_2025_02_07!08_40_41_AM.pdf

24. Book 1 - Foundation of Digital Forensics. 196 p. URL: https://ec.europa.eu/programmes/erasmus-plus/project-result-content/2a54509d-b6bb-43d8-8250-eae26782c392/FORC%20Book%201.pdf

25. Book 2 - Digital Forensic Procedures. 118 p. URL: https://ec.europa.eu/programmes/erasmus-plus/project-result-content/d7359393-291d-4f43-8abe-1211ff80d86e/FORC_Book_2.pdf

26. Kemal Hajdarevic, Nermin Ziga, Mirza Halilovic. Essentials of Digital Forensics. Sarajevo, 2019. 165 p. URL: https://shorturl.at/v4v4X

27. Bill Nelson, Amelia Phillips, Christopher Steuart. Guide to Computer Forensics and Investigations: Processing Digital Evidence. Sixth Edition. Copyright 2019 Cengage Learning. 738 p. URL: https://klikitscripts.com/toddbooks/files/computer%20forensics%20file.pdf

28. Якимчук М. Ю. Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект. Нове українське право. 2021. № 4. С. 182-186. DOI: https://doi.org/10.51989/NUL.2021.4.27 (дата звернення: 24.08.2025).

29. Діброва Т.А., Пісенко Д.О., Сметаніна Н.В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. юридичний науковий електронний журнал. 2022. № 11. С. 546-549. DOI: https://doi.org/10.32782/2524-0374/2022-11/132 (дата звернення: 21.08.2025).

30. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса : Національний університет «Одеська юридична академія», 2020. 112 с. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0053461.pdf.

31. Бодунова О.М. Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій. *Аналітично-порівняльне правознавствою,* 2023. № 1. DOI:: https://doi.org/10.24144/2788-6018.2023.01.76 (дата звернення: 24.08.2025).

32. Семенюк О. О. До питання про міжнародно-правове розуміння кіберзлочину. *Європейський правничий часопис*. 2023. №1. С. 117-121.

33. Попко В. В., Попко Є. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського Національного Університету: Серія ПРАВО.* 2021. Випуск 66. С. 276-283. DOI: https://doi.org/10.24144/2307-3322.2021.66.46 (дата звернення: 24.08.2025).

34. Неділко Я. Поняття цифрової криміналістики та її місце в системі криміналістики. *Criminalistics and Forensics*..2025.. DOI: 10.33994/kndise.2024.69.21 (дата звернення: 24.08.2025).

35. Редька Я. О. Цифрова криміналістика: виклики, методи та перспективи в сучасних умовах // VII Міжнародний молодіжний науковий юридичний форум: [Матеріали форуму, м. Київ, Національний авіаційний університет, 16-17 травня 2024 р.]. С.287-290.

36. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2022. Вип. 3 (99). С. 283-294.

37. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права : наук. журн.* 2022. № 1. С. 176–180.

38. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Том 4. № 85. С. 71-75. DOI: https://doi.org/10.24144/2307-3322.2024.85.4.10 (дата звернення: 21.08.2025).

39. Demydova, Y. Trends in the Development of Digital Forensics: Challenges and Prospects for Criminal Justice Agencies. *Problems of Legality*. 2025.. №168. P. 164–182. DOI: https://doi.org/10.21564/2414-990X.168.32499 (date of access: 25.08.2025).

40. Tiapkin A., Lushchyk I. Problematic Issues of Definition of Digital Forensics. Theory and Practice of Jurisprudence. 2024. №1(23). C. 135–161. DOI: https://doi.org/10.21564/2225-6555.2023.23.281734 (date of access: 25.08.2025)..

41. Lena Klasen, Niclas Fock, Robert Forchheimer. The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International.* 2024. Volume 362. DOI: https://doi.org/10.1016/j.forsciint.2024.112133 (date of access: 25.08.2025).

42. Christopher Hargreaves, Alex Nelson, Eoghan Casey. An abstract model for digital forensic analysis tools - A foundation for systematic error mitigation analysis. *Forensic Science International: Digital Investigation.* 2024. Volume 48. DOI: https://doi.org/10.1016/j.fsidi.2023.301679 (date of access: 25.08.2025).

43. Noland Alec. Current Challenges of Digital Forensics. *Themis: Research Journal of Justice Studies and Forensic Science.* 2024. Vol. 12 : Iss. 1 , Article 1. DOI: https://doi.org/10.55917/2324-6561.1120 (date of access: 25.08.2025).

44. Zareen M. S., Aslam B., Tahir S., Rasheed I., Khan F. Unveiling the Dynamic Landscape of Digital Forensics: The Endless Pursuit. *Computers.* 2024. №13(12), 333. DOI: https://doi.org/10.3390/computers13120333 (date of access: 25.08.2025).

45. Selim Aybeyan, Ali Ilker. The Role of Digital Forensic Analysis in Modern Investigations. *Journal of Emerging Computer Technologies*. 2024. № 4. P 1-5.

46. AlKhanafseh M., Surakhi O. Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography. *Electronics*. 2024. №13(18), 3729. DOI: https://doi.org/10.3390/electronics13183729 (date of access: 25.08.2025).

13. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=8033

2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/

3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home

ЦИФРОВА КРИМІНАЛІСТИКА

Тип дисципліни	Вибіркова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	–
Кількість призначених кредитів ЄКТС	8,0
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен: *знати* теоретичні основи і сучасні інформаційні технології аналізу та збору цифрової криміналістичної інформації; *вміти* застосовувати методи цифрової криміналістики; досліджувати дані і визначити джерела даних; *вміти* отримувати і описувати цифрові докази; застосовувати способи аутентифікації цифрових доказів; *вміти* порівнювати і зіставити цифрові докази і традиційні докази для встановлення відмінностей між ними; *використовувати і критично аналізувати* моделі процесів цифрової криміналістики; *застосовувати* національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів; *застосовувати* стандарти і передові практичні методи, що стосуються цифрових доказів в цифровій криміналістиці; *володіти* основними поняттями, методами та інструментами цифрової криміналістики; володіти навичками збору і аналізу цифрової криміналістичної інформації, способами аутентифікації цифрових доказів; *володіти* умінням самостійно опановувати нові методи та технології розслідування кіберзлочинів та запобігання кіберзлочинам.

Зміст навчальної дисципліни. Вступ до науки цифрової криміналістики (DFS), основні поняття і визначення цифрової криміналістики. Основи комп'ютерної грамотності фахівця з DFC. Докази цифрової криміналістики, розташування та види доказів. Цифрові (електронні) докази. Принцип обміну та збір доказів на місці злочину. Інструменти цифрової криміналістики. Проведення досліджень. Розділи цифрової криміналістики: Криміналістика хостів, Криміналістика електронної пошти і миттєвих повідомлень, Мережева криміналістика, Криміналістика мобільних пристроїв. Антикриміналістика в розрізі технік і операційних систем, Антикриміналістика файлових структур, Стеганографія і стеганоаналіз в цифровій криміналістиці. Моделі розслідування, Експертиза й аналіз. Правові та етичні аспекти в цифровій криміналістиці. Міжнародна організація з комп'ютерних доказів (International Organization on Computer Evidence –IOCE) та Наукова робоча група по дослідженню цифрових доказів (Scientific Working Group on Digital Evidence – SWGDE).

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для ***другого*** (магістерського) рівня вищої освіти за денною формою здобуття освіти становить 8 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних та наочних методів, мультимедійних технологій, проблемного й інтерактивного навчання, мотиваційних прийомів); лабораторні заняття (з використанням частково-пошукових і контекстних методів, аналізу проблемних ситуацій, розвитку критичного мислення, пояснення, елементів дискусії тощо); самостійна робота (опрацювання програмного матеріалу з відповідних джерел інформації, підготовка до виконання і захисту лабораторних робіт, тестування тощо), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт; тестування.

Вид семестрового контролю: залік.

Навчальні ресурси:

1. Вступ до цифрової криміналістики : навч. посіб. / В. Ю. Шепітько та ін. ; за ред. В. Ю. Шепітька. Харків : Право, 2025. 124 с.

2. Кіберзлочинність та електронні докази : навч. посібник / Б. М. Головкін та ін. ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

3. Степанюк Р. Л., Гусєва В. 0. Сучасні криміналістичні засоби та методи протидії злочинності: навч. посіб. Харків : ХНУВС, 2024. 232 с.

4. Joakim Kavrestad, Marcus Birath, Nathan Clarke. Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications. Third Edition. Springer, 2024. 297 p.

5. Suhas Pednekar, Ravindra D. Kulkarni, Prakash Mahanwar. Cyber forensics. Published by Director Institute of Distance and Open Learning, University of Mumbai, Vidyanagari, Mumbai - 400 098, 2022. 275 p.

6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=8033

7. Електронна бібліотека ХНУ. Доступ до ресурсу: http://library.khmnu.edu.ua/

Викладачі: канд. техн. наук, доцент Чешун В.М.