ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету IT
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«____» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Цифрова криміналістика

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Рівень вищої освіти	Другий магістерський
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	8 кредитів ЄКТС
Шифр дисципліни	ОПП.05
Мова навчання	**у**країнська
Статус дисципліни	вибіркова
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни	Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
				Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	-	-	8	240	34	51			155			+	

Робоча програма складена _____ канд.техн.наук, доцент Віктор ЧЕШУН
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО .
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

ЦИФРОВА КРИМІНАЛІСТИКА

Тип дисципліни	Вибіркова
Освітній рівень	Другий (магістерський)
Мова викладання	Українська
Кількість кредитів ЄКТС	8
Форми здобуття освіти	Очна денна

Результати навчання. Студент, який успішно завершив вивчення дисципліни, 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. Основи цифрової криміналістики. Цифрова криміналістика операційних систем. Комп'ютерні злочини та інциденти. Розслідування цифрових злочинів. Оперативно-розшукові заходи і слідчі дії. Збір і класифікація доказів. Експертиза доказів. Міжнародна організація з комп'ютерних доказів. Використання нормативно-правового забезпечення в цифровій криміналістиці.

Запланована аудиторна робота: кількість аудиторних годин – не менше 1/3 від загальної кількості годин, які заплановані для вивчення дисципліни.

Методи навчання: словесні, наочні та інтерактивні (лекції); практичні (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Форми оцінювання результатів навчання: захист лабораторних робіт, тестування.

Форма семестрового контролю: залік.

Навчальні ресурси:

1. Digital Forensics Basics: A Practical Guide Using Windows OS/ Edited by Nihad A. Hassan. New York, 2019. 335 p.
2. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник /О.А. Самойленко. Одеса, 2020. 112 с.
3. Кіберзлочини в Україні (кримінально-правова характеристика): навч. посіб. Луцьк: СПД Гадяк Ж. В. друкарня «Волиньполіграф»™, 2019. 304 с.
4. Digital Forensics / Edited by André Årnes. John Wiley & Sons Ltd, 2018. 336 p.
5. Cybercrime: University Module Series, Teaching Guide/ United Nations Office on Drugs and Crime. Vienna, United Nations, Doha Declaration, 2019. 453 p.
6. Hemdan, E.ED., Manjaiah, D. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimed Tools Appl 80, 14255–14282 (2021).
7. Solanke, A.A., Biasiotti, M.A. Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. Künstl Intell 36, 143–161 (2022).
8. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/.
9. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.

Викладач: к.т.н., доцент Чешун В.М.

ВСТУП

Дисципліна «Цифрова криміналістика» – вибіркова складова професійної підготовки магістрів в галузі інформаційних технологій зі спеціальності „Кібербезпека”, що 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. Поглиблення теоретичної і практичної підготовки фахівця, спрямованої на вирішення типових та складних завдань цифрової криміналістики, що полягають у зборі цифрової криміналістичної інформації, збереженні, дослідженні і використанні цифрових доказів.

Предмет дисципліни. Основи цифрової криміналістики, цифрова криміналістики операційних систем; комп'ютерні злочини та інциденти, розслідування, оперативно-розшукові заходи і слідчі дії, збір і класифікація доказів, експертиза доказів, міжнародна організація з комп’ютерних доказів, використання нормативно-правового забезпечення в цифровій криміналістиці.

Завдання дисципліни. Сформувати знання про принципи, що лежать в основі цифрової криміналістики, методи і засоби пошуку цифрових доказів, технології розслідування кіберзлочинів. Вивчення дисципліни має забезпечити набуття компетентностей та досягнення результатів навчання:

компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях

КЗ 2. Знання та розуміння предметної області та розуміння професії

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

Фахові компетентності

КФ 4. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, безпеки інформаційних технологій (в т.ч. хмарних технологій та додатків), а також безпеки бізнес/операційних процесів з метою забезпечення функціонування інформаційно-комунікаційних систем згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

результати навчання:

РН 1. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН 2. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН 3. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації.

РН 4. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

РН 5. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

РН 6. Вирішувати задачі збору, збереження, аналізу і інтерпретації цифрових доказів.

Студент, який успішно завершив вивчення дисципліни, 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.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин, відведених на:		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Вступ до науки цифрової криміналістики (DFS)	4	6	18
Тема 2. Основи комп'ютерної грамотності фахівця з DFC	6	6	20
Тема 3. Докази цифрової криміналістики	2	-	5
Тема 4. Місце злочину	8	30	68
Тема 5. Розділи цифрової криміналістики	8	-	16
Тема 6. Антикриміналістика	4	6	14
Тема 7. Експертиза й аналіз	2	3 (4/2)*	14 (13/15)*
Разом:	**34**	**51** (52/50)*	**155** (154/156)*

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
Тема 1. Вступ до науки цифрової криміналістики (DFS)		
1	**Введення в цифрову криміналістику.** 1. Вступ до цифрової криміналістики 2. Визначення цифрової криміналістики 3. Наука цифрової криміналістики 4. Спільноти у сфері цифрової криміналістики 5. Цифрова криміналістика, Кіберкриміналістика чи Комп'ютерна криміналістика? 6. Визначення цифрової криміналістики – паразитуючі міфи і вплив медіа. Літ.: [1] с.3-17, с.33-39, с.57-61; [22] с.29-70.	2
2	**Основні поняття і визначення цифрової криміналістики.** 1. Контекст цифрової криміналістики 2. Заходи кіберкриміналістики 3. Цифрова криміналістика в різних контекстах 4. Науковий підхід в цифровій криміналістиці 5. Підсумок за темою 1 Літ.: [6] с.26-50; [7] с.17-27.	2
Тема 2. Основи комп'ютерної грамотності фахівця з DFC		
3	**Жорсткі диски – фізична і логічна організація** 1. Основи комп'ютерної грамотності – цілі навчання 2. Основні типи дисків 3. Жорсткий диск (HDD) порівняно із твердотілим накопичувачем (SSD) 4. Структури жорсткого диска (HDD) 5. Розрахунок ємності накопичувача 6. Адресація жорсткого диска Літ.: [2] с.153-156.	2
4	**Розбиття (поділ) диска** 1. Розбиття або поділ диска на розділи і типи форматів 2. Головна таблиця розділів 3. Коди типів розділу, hex-коди типів розділу 4. Варіанти розбиття (поділу) диска 5. Приховані розділи 6. Область, захищена хостом (HPA) 7. Оверлей конфігурації диска (DCO) Літ.: [2] с.156-159	2
5	**Процес завантаження** 1. Процес завантаження – основні поняття 2. Процес завантаження – формат для старіших версій (Legacy) 3. Процес завантаження – UEFI 4. Процес завантаження – Windows UEFI 5. Процес завантаження - POST 6. Процес завантаження Windows 10 7. Процес завантаження Linux 8. Процес завантаження Unix 9. Процес завантаження Mac OS 11 Літ.: [2] с.159-190.	2

Тема 3 – Докази цифрової криміналістики		
6	**Розташування та види доказів** 1. Види цифрових доказів 2. Розташування доказів 3. Розташування доказів – електронна пошта 4. Розташування доказів – принтери 5. Розташування доказів – пристрої Roku, медіаплеєри Fire Sticks 6. Розташування доказів – маршрутизатори (роутери) 7. Розташування доказів – Raspberry Pi (одноплатні комп'ютери) 8. Геолокація 9. Фото і відео 10. EXIF (Exchangeable Image File Format – придатний до обміну формат файлів зображень) [Метадані] 11. Місцеположення iPhone 12. Геолокація IP 13. Місця розташування за соціальними мережами 14. Теги геолокації за соціальними мережами 15. Розташування стільникових веж Літ.: [2] с.13-48; [5]	2
Тема 4. Місце злочину		
7	**Принцип обміну та збір доказів на місці злочину** 1. Принцип обміну 2. Що таке місце злочину? 3. Докази 4. Принципи криміналістики 5. Виявлення цифрових (електронних) доказів 6. Процедури, яких слід дотримуватися на місці злочину 7. Контрольний список, обґрунтований з погляду криміналістики 8. Набори для роботи експерта-криміналіста на виїзді Літ.: [2] с.61-84.	2
8	**Цифрові (електронні) докази** 1. Цифрові (електронні) докази - 2. Вилучення та збереження доказів 3. Докази на комп'ютері 4. Докази на телефоні 5. Докази у хмарних сховищах 6. Докази в мережі 7. Середовище, що стосується розслідування (IE) 8. IE – Техніки 9. IE – Міркування Дауберта 10. IE – Інструменти 11. IE – Технології 12. IE – Автоматизація 13. IE – Планування Літ.: [2] с.39-40; [10] с.33-64	2
9	**Інструменти цифрової криміналістики** 1. Стислий огляд інструментів цифрової криміналістики 2. Апаратні блокувальники запису 3. Програмні блокувальники запису 4. Чому використовуються образи/зображення 5. Побітова копія (копія бітового потоку) порівняно з резервною копією 6. Криміналістичний образ (зображення): Фізичний диск	2

	7. Криміналістичний образ (зображення) логічного тому 8. Хеш-функція MD5 для цілісності образу (зображення) даних 9. Огляд програмного забезпечення для створення образів 10. Програмне забезпечення для створення образів – FTK Imager 11. Мобільні системи для роботи експерта-криміналіста на виїзді (MFS) 12. Вимоги до інструментів для створення образів дисків 13. Набори для роботи експерта-криміналіста на виїзді Літ.: [3] с.19-33	
10	**Проведення досліджень (експертиза)** 1. Криміналістичне мислення 2. Хронологія подій у рамках розслідування 3. MAC times (частини метаданих файлової системи) 4. Організація проведення розслідування 5. Запитання в рамках розслідування 6. Модель проведення експертизи доказів у цифровій криміналістиці 7. Запитання в рамках розслідування – Заитання/Запити 8. Реєстр Windows 9. HKEY_CLASSES_ROOT 10. Інструменти реєстру 11. Файли ntuser.dat та index.dat 12. Інструменти управління провадженнями Літ.: [2] с.61-84; [10] с.164-267	2
Тема 5. Розділи цифрової криміналістики		
11	**Криміналістика хостів** 1. Криміналістика хостів – об'єкти 2. Криміналістика хостів 3. Криміналістика хостів – віртуальні машини Літ.: [2] с. 275-314 ; [4] с. 119-131	2
12	**Криміналістика електронної пошти і миттєвих повідомлень** 1. Криміналістика електронної пошти і миттєвих повідомлень- введення 2. Криміналістика електронної пошти і миттєвих повідомлень 3. Розслідування електронної пошти Літ.: [2] с. 275-314 ; [4] с. 119-131	2
13	**Мережева криміналістика** 1. Що таке мережева криміналістика? 2. Основи криміналістичного аналізу мережі 3. Атаки мережі 4. Які докази можна зібрати? 5. Інструменти мережевої криміналістики 6. Що слід запам'ятати для успіху мережевої криміналістики Літ.: [4] с. 133-144	2
14	**Криміналістика мобільних пристроїв** 1. Криміналістика мобільних пристроїв - введення 2. Криміналістика мобільних пристроїв і Геді Ламар 3. Перелаштування частоти 4. CDMA 5. Мобільні телефони в історії 6. Що нас цікавить? Види доказів 7. Криміналістика мобільних пристроїв та вбудованих систем як наука 8. Синергія Літ.: [2] с. 191-274; [4] с. 145-161	2

Тема 6. Антикриміналістика		
15	**Антикриміналістика в розрізі технік і операційних систем** 1. Поширені техніки 2. Антикриміналістика 3. Область свопінгу 4. Антикриміналістика Windows 5. Антикриміналістика FS Unix 6. Зарезервований простір 7. Альтернативні потоки даних (ADS) 8. Підсумки щодо приховання даних Літ.: [4] с. 83-103	2
16	**Антикриміналістика файлових структур. Стеганографія і стеганоаналіз** 1. Видалення, переформатування та сміттєвий кошик 2. Зберігання файлів у NTFS 3. Видалені файли 4. Видалення файлу 5. Надсилання в кошик / видалення каталогу 6. Видалені файли у NTFS 7. Заповнювачі 8. Файл INFO2 9. Desktop.ini 10. Стеганографія 11. Стеганоаналіз 12. Інструменти для виявлення слідів стеганографії Літ.: [4] с. 83-103	2
Тема 7. Експертиза й аналіз		
17	**Експертиза й аналіз** 1. Моделі розслідування 2. ADFM 3. IDIP 4. EIDIP 5. HOBFDIP 6. Критика моделей 7. Аналіз цифрового місця злочину 8. Якісна криміналістична процедура 9. Аналіз категорій 10. Вимоги до аналітичних інструментів 11. Атрибуція – поняття і фази. 12. Підходи Ческі. 13. Сценарії атрибуції 14. Виклики атрибуції. 15. Підсумок лекції Літ.: [4] с.27-36, [5]	2
	Разом:	**34**

Зміст лабораторних робіт

№ з/п	Тема лабораторного заняття	Кількість годин
1	Збір та аналіз цифрової криміналістичної інформації засобами операційної системи Літ.: [2] с. 185-190; [4] с. 65-82	6
2	Отримання цифрової криміналістичної інформації, заблокованої парольною аутентифікацією. Літ.: [1] с. 24-29	6
3	Відновлення прихованої та знищеної цифрової криміналістичної інформації на накопичувачах різних видів. Літ.: [2] с. 147-184	6
4	Збір та аналіз цифрової криміналістичної інформації програмою для електронної експертизи FTK. Літ.: [4] с. 38-46	6
5	Збір та аналіз цифрової криміналістичної інформації з носіїв даних програмою Autopsy. Літ.: [2] с. 34-49	6
6	Збір та аналіз цифрової криміналістичної інформації в мережі Internet. Літ.: [2] с. 275-314 ; [4] с. 119-131	6
7	Збір та аналіз цифрової криміналістичної інформації з мобільних пристроїв засобами Wondershare Dr.Fone for Android Літ.: [2] с. 191-274; [4] с. 145-161	6
8	Антикриміналістика інструментами стеганографії Літ.: [4] с. 83-103	6
9	Підсумкове заняття. Тестування.	3 (4/2)*
	Разом:	**51** (52/50)*

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

Зміст самостійної (у т.ч. індивідуальної) роботи

На самостійне опрацювання студентів виноситься опрацювання лекційного матеріалу, підготовка до виконання і захисту лабораторних робіт. Керівництво самостійною роботою та виконанням завдань здійснює викладач згідно з розкладом консультацій в позаурочний час, в тому числі із застосуванням технологій інтерактивного та дистанційного навчання.

Номер тижня	**Вид самостійної роботи**	**Кількість годин**
1	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР1	9
2	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР1	9
3	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР2	9
4	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР2	9
5	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР3	9
6	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР3. Підготовка до тестування	10
7	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР4	9
8	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР №4	9
9	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР5	9
10	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР5	9
11	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР6	9
12	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР6	9
13	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР7	9
14	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР7	9
15	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР8	9
16	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8	9
17	Опрацювання теоретичного матеріалу. Підготовка до підсумкового заняття і тестування	10 (9/11)*
	Разом:	**155** (154/156)*

Умовні позначення: ЛР – лабораторна робота

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу лабораторнх занять)

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів, зокрема: лекції з використанням словесних, наочних та інтерактивних методів і візуалізації (лекції); лабораторні роботи з використанням практичних, проблемних, продуктивних методів, тренінгових майстер-класів, самостійна робота передбачає пояснювально-ілюстративні та дослідницькі методи.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: виконання частини лабораторних робіт передбачає роботу у малих групах з призначенням тім-лідера, що сприяє розвитку лідерських якостей у студентів, здатності до спілкування і організації командної роботи над спільними задачами, а змінюваність складу робочих груп між лабораторними роботами сприяє розвитку навичок адаптованості, гнучкості, комунікативності і оперативного налагоджування міжособистісних відносин в різних колективах; спілкування з проблемних питань під час лекцій, прилюдні захисти лабораторних робіт з обгрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни, що передбачає рішення проблемних завдань із застосуванням творчих підходів; обмежений час на виконання лабораторних робіт і тестових завдань, чітко визначені терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

Необхідні інструменти, обладнання, програмне забезпечення: ПК з підключенням до локальної мережі та мрежі Internet, операційні системи (Windows, Kali Linux тощо), програми збору цифрової криміналістичної інформації (FTK, Autopsy, Wondershare Dr.Fone for Android).

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторної роботи;
- тестування.

При виведенні підсумкової семестрової оцінки враховуються результати поточного контролю (залік за рейтингом формується автоматично за результатами поточного контролю).

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

Аудиторна робота			**Контрольні заходи**	**Підсумковий контрольний захід**
Лабораторні роботи №:		Тестовий контроль 1	Тестовий контроль 2	Семестровий контроль
1 - 8		Т 1-3	Т 4-7	Залік
ВК:	0,8	0,2	0,2	

<u>Оцінювання лабораторних робіт</u>. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день

виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з п'ятнадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 15.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–5	6–10	11–13	14–15
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 15 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в онлайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
1	*2*
Відмінно	Студент 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 державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, 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 закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент 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 студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, 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	Студент 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 студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані

терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно”.

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**		
A	4,75–5,00	5	Зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незарахо-вано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ 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.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни „Цифрова криміналістика” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Цифрова криміналістика : консп. лекцій / уклад. І. З. Якименко. - Тернопіль : ТНЕУ, 2019. - 109 с.
2. Digital Forensics / Edited by André Årnes. – John Wiley & Sons Ltd, 2018. – 336 p.
3. Cybercrime: University Module Series, Teaching Guide. / United Nations Office on Drugs and Crime. ¬¬– Vienna, United Nations, Doha Declaration, 2019. – 453 p.
4. Digital Forensics Basics: A Practical Guide Using Windows OS/ Edited by Nihad A. Hassan. – New York, 2019. – 335 p.
5. Самойленко О. А. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник / О. А. Самойленко. Одеса : , 2020. 112 с.
6. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – Видання друге, перероб. та доп. – Одеса : ОНАЗ ім. О.С. Попова, 2019. − 320 с.
7. Комп’ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. – Київ: «Центр учбової літератури», 2018. – 558 с
8. Баранник В. В. Основы теории структурно-комбинаторного стеганографического кодирования: монография / В. В. Баранник, А. Э. Бекиров, Д. В. Баранник. – Х. : ХНУРЕ, 2017. - 256 с
9. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
10. The Basics of Digital Forensics The Primer for Getting Started in Digital Forensics. Second Edition / John Sammons. – Elsevier Inc., 2015. – 180 p.
11. Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с.
12. Practical Information Security: A Competency-Based Education Course / [Izzat Alsmadi, Robert Burdwell, Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Ali Al-Qudah, Ahmad Al-Omari]. – Cham, Switzerland : Springer International Publishing AG, 2018. – 328 p.
13. Про національну безпеку України: Закон України [Електронний ресурс] / Затверджено Указом Президента України від 21 червня 2018 року № 2469^Ш – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19. – Назва з екрану.
14. Стратегія кібербезпеки України [Електронний ресурс] / Указ Президента України від 15.01.2016 р. № 96/2016 – Режим доступу:. https://zakon5.rada.gov.Ua/laws/show/96/2016#n11. – Назва з екрану.
15. Стратегія національної безпеки України [Електронний ресурс] / Указ Президента України від 06.05.2015р. № 287/2015 – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015. – Назва з екрану.

Додаткова

16. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. МЕТОДИ ЗАХИСТУ. Настанови щодо кібербезпеки. – Чинний від 2016-27-12. – Київ : ДП «УкрНДНЦ», 2018. – [50] с.
17. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
18. Поняття та класифікація віртуальних слідів кіберзлочинів // Я. Найдьон. / Криміналістика. – 2019. – №5. – С. 304-307.

19. Проблеми застосування інформаційних технологій правоохоронними структурами України та закладами вищої оевітм зі специ* фінними умовами навчання : збірник наукових етатей за матеріалами доповідей Всеукраїнської науково-практичної конференції 21 грудня 2018 року / упорядник Т. В. Маїеровська / - Львів: ЛьвДУВС, 2018.-281 с.

20. Авдєєва Г. К. Сутність цифрових слідів в криміналістиці / Г. К. Авдєєва // Актуальні питання судової експертизи та криміналістики : зб. матеріалів міжнар. наук.-практ. конфер., присвяч. 95-річчю створення Харків. НДІ суд. експертиз ім. засл. проф. М. С. Бокаріуса (Харків, 10–11 жовт. 2018 р.). – Харків, 2018. – С. 90–93.

21. Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service // Xiaoyu Du, Nhien-An Le-Khac, Mark Scanlon / 16th European Conference on Cyber Warfare and Security (ECCWS 2017) At: Dublin, Ireland, June 2017. – P. 46-57.

22. Шеломенцев В. П. Віртуальність як елемент характеристики кіберзлочинів / В. П. Шеломенцев / Часопис Національного університету "Острозька академія". Серія "Право". – 2011. – №1(3). – С. 1-15

23. Cybersecurity: Geopolitics, Law, and Policy / Amos N. Guiora; Professor of Law at the S.J. Quinney College of Law, University of Utah, USA. – New York : Taylor & Francis Books, 2017. ¬– 177 p.

24. Гладун А.Я. Таксономія стандартів інформаційної безпеки / А.Я. Гладун, К.О. Хала // Наука, технології, інновації. – 2017. – № 2. – С. 53-64

25. Shojaie B. Implementation of Information Security Management Systems based on the ISO/IEC 27001 / Bahareh Shojaie. - Dissertation with the aim of achieving a doctoral degree at the Faculty of Mathematics, Informatics and Natural Sciences Department of Informatics of Universit¨at Hamburg. February 20, 2018. 147 p.

26. Кондратенко Ю. В. Візуальний аналіз політик безпеки в ERP-системах / Ю. В. Кондратенко, І. Г. Зотова, В. В. Грицюк // Збірник наукових праць Центру воєнно-стратегічних досліджень НУ оборони України ім. Івана Черняховського. – 2018. – № 1. – С. 68-73.

27. Stevens C. Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet / Clare Stevens // Contemporary Security Policy. – 2020. – Volume 41, Issue 1: Special issue: Cyber Security Politics. – P. 129-152.

28. Овсяннiков В. В. Аналіз нормативно-правових та організаційно-технічних аспектів забезпечення інформаційної безпеки / [В. В. Овсяннiков, С. В. Дехтяр, С. А. Паламарчук, Ю. О. Черниш, О. В. Шемендюк]. // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – № 3(24). – С. 187-193.

29. Борсуковський Ю. В. Визначення сучасних вимог до створення політики управління доступом корпоративних користувачів / Ю. В. Борсуковський // Сучасний захист інформації. – 2016. – № 4. – С. 5-9.

30. Борсуковський Ю. В Визначення сучасних вимог щодо політики використання засобів криптографічного захисту інформації на підприємстві / Ю. В. Борсуковський // Сучасний захист інформації. – 2018. – № 1. – С. 74-81.

31. Ахрамович В. М. Адміністративний рівень інформаційної безпеки / В. М. Ахрамович // Сучасний захист інформації. – 2017. – № 1. – С. 10-14.

32. Dunn M. Cyber security meets security politics: Complex technology, fragmented politics, and networked science / Myriam Dunn Cavelty, Andreas Wenger // Contemporary Security Policy. – 2020. – Volume 41, Issue 1: Special issue: Cyber Security Politics. – P. 5-32.

33. Hend K. Alkahtani. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions / Hend K. Alkahtani // Computer and Information Science. – Vol. 12, No. 2; 2019. – ISSN 1913-8989, E-ISSN 1913-8997. – Published by Canadian Center of Science and Education. – P. 117-125.

34. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол.: В. Ю. Шепітько (голов. ред.), В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. – Харків : Право, 2019. – 164 с.

35. Digital forensic readiness framework based on honeypot and honeynet for byod // Audrey Asante, Vincent Amankona. / Journal of Digital Forensics. – Vol. 16 (2021). – P. 1-17.

36. Forensic of an unrooted mobile device // Animesh Kumar Agrawal, Aman Sharma, Sumitra Ranjan Sinha and Pallavi Khatri / International Journal of Electronic Security and Digital Forensic. – 2019. – Vol. 12, No. 1 – P. 118-137.

37. Russia Today, Cyberterrorists Tomorrow: U.S. Failure to Prepare Democracy for Cyberspace // Jonathan F. Lancelot, Norwich UniversityFollow / Journal of Digital Forensics. – Vol. 13 (2018). – P. 23-32.

38. Application of quality in use model to assess the user experience of open source digital forensics tools // Manar Abu Talib, Reem Alnanih and Adel Khelifi / International Journal of Electronic Security and Digital Forensic. – 2019. – Vol. 12, No. 1 – P. 43-76.

39. A Two-Stage Model for Social Network Investigations in Digital Forensics // Anne David, Sarah Morris, Gareth Appleby-Thomas. / Journal of Digital Forensics. – Vol. 15 (2020). – P. 1-36.

40. Hemdan, E.ED., Manjaiah, D. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimed Tools Appl 80, 14255–14282 (2021).

41. Solanke, A.A., Biasiotti, M.A. Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques. Künstl Intell 36, 143–161 (2022).

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua/.

2. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/.