ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
Тетяна ГОВОРУЩЕНКО
«31» серпня 2024 р.

СИЛАБУС

Навчальна дисципліна: «*Цифрова криміналістика*»

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: другий (магістерський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Чешун Віктор Миколайович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/cheshun-viktor-mykolajovych/
E-mail викладача(ів)	cheshunvn@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=8033
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/8577265687 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр І (осінньо-зимовий)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

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	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
ОД	-	-	8	240	85	34	51			155			+	

Анотація дисципліни

Дисципліна «Цифрова криміналістика» є вибірковою, викладається для студентів очної денної форми навчання, рекомендована для здобувачів вищої освіти за освітньо-професійною програмою «Кібербезпека та захист інформації» другого (магістерського) рівня. При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити – немає.

Кореквізити – немає.

Мета і завдання дисципліни

Мета дисципліни. Формування системи знань та розуміння основних понять та методів цифрової криміналістики, навиків збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем Windows та Linux, спеціалізованого програмного забезпечення і технічних засобів.

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: *вміти* застосовувати методи цифрової криміналістики; досліджувати дані і визначити джерела даних; отримувати і описувати цифрові докази; застосовувати способи аутентифікації цифрових доказів; 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 в сфері кібербезпеки; застосовувати стандарти і передові практичні методи, що стосуються цифрових доказів в цифровій криміналістиці. *володіти* основними поняттями, методами та інструментами цифрової криміналістики; навичками збору і аналізу цифрової криміналістичної інформації; способами аутентифікації цифрових доказів; умінням самостійно опановувати нові методи та технології розслідування кіберзлочинів та запобігання їм.

Тематичний і календарний план вивчення дисципліни

Номер тижня	Тема лекції*	Тема лабораторної роботи**	Самостійна робота студента		
			Зміст	Години	Літера-тура
1	*3*	*4*	*5*	*6*	*7*
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.	Підгрупа 1: **Збір та аналіз цифрової криміналістичної інформації засобами операційної системи**	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №1.	9	[1] с.3-17, с.33-39, с.57-61; [22] с.29-70. [2] с. 185-190; [4] с. 65-82
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	Підгрупа 2: **Збір та аналіз цифрової криміналістичної інформації засобами операційної системи**	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №1.	8	[6] с.26-50; [7] с.17-27 [2] с. 185-190; [4] с. 65-82
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	Підгрупа 1: **Отримання цифрової криміналістічної інформації, заблокованої парольною аутентифікацією.**	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №2.	9	[2] с.153-156 **[1] с. 24-29**
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 диска 5. Приховані розділи 6. Область, захищена хостом (HPA) 7. Оверлей конфігурації диска (DCO)	Підгрупа 2: **Отримання цифрової криміналістічної інформації, заблокованої парольною аутентифікацією.**	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №2.	8	[2] с.156-159 **[1] с. 24-29**

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	Підгрупа 1: **Відновлення прихованої та знищеної цифрової криміналістічної інформації на накопичувачах різних видів.**	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №3.	9	[2] с.159-190 **[2] с. 147-184**
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	Підгрупа 2: **Відновлення прихованої та знищеної цифрової криміналістічної інформації на накопичувачах різних видів.**	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №3.	8	[2] с.13-48; [5] **[2] с. 147-184**
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	Підгрупа 1: **Збір та аналіз цифрової криміналістичної інформації програмою для електронної експертизи FTK.**	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №4.	9	[2] с.61-84 [4] с. 38-46

	8. Набори для роботи експерта-криміналіста на виїзді				
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	Підгрупа 2: **Збір та аналіз цифрової криміналістичної інформації програмою для електронної експертизи FTK.**	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №4.	8	[2] с.39-40; [10] с.33-64
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 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	Підгрупа 1: **Збір та аналіз цифрової криміналістичної інформації з носіїв даних програмою Autopsy.**	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №5.	9	[3] с.19-33 [2] с. 34-49
10	**Проведення досліджень (експертиза)** 1. Криміналістичне мислення 2. Хронологія подій у рамках розслідування 3. MAC times (частини метаданих файлової системи)	Підгрупа 2: **Збір та аналіз цифрової криміналістичної інформації з носіїв даних програмою Autopsy.**	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №5.	8	[2] с.61-84; [10] с.164-267 [2] с. 34-49

	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				
11	**Криміналістика хостів** 1. Криміналістика хостів – об'єкти 2. Криміналістика хостів 3. Криміналістика хостів – віртуальні машини	Підгрупа 1: **Збір та аналіз цифрової криміналістичної інформації в мережі Internet.**	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №6.	9	[2] с. 275-314 ; [4] с. 119-131
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	Підгрупа 2: **Збір та аналіз цифрової криміналістичної інформації в мережі Internet.**	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №6.	8	[2] с. 275-314 ; [4] с. 119-131
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	Підгрупа 1: **Збір та аналіз цифрової криміналістичної інформації з мобільних пристроїв засобами Wondershare Dr.Fone for Android**	Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №7.	9	[4] с. 133-144 [2] с. 191-274; [4] с. 145-161
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	Підгрупа 2: **Збір та аналіз цифрової криміналістичної інформації з мобільних пристроїв засобами Wondershare Dr.Fone for Android**	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №7.	8	[2] с. 191-274; [4] с. 145-161
15	**Антикриміналістика в розрізі технік і операційних систем** 1. Поширені техніки	Підгрупа 1: **Антикриміналістика інструментами**	Опрацювання теоретичного матеріалу.	9	[4] с. 83-103

	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	**стеганографії**	Підготовка до виконання лабораторної роботи №8.		
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	Підгрупа 2: **Антикриміналістика інструментами стеганографії**	Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №8.	8	[4] с. 83-103
17	**Експертиза й аналіз** 1. Моделі розслідування • ADFM • IDIP • EIDIP • HOBFDIP 2. Критика моделей 3. Аналіз цифрового місця злочину 4. Якісна криміналістична процедура 5. Аналіз категорій 6. Вимоги до аналітичних інструментів 7. Підсумок лекції	Підгрупа 1: **Підсумкове заняття. Тестування**	Опрацювання теоретичного матеріалу. Підготовка до підсумкового тестування.	7	[5]

* лекції проводяться щотижня по 2 години;

** лабораторні роботи проводяться раз у два тижні по 6 годин.

Політика дисципліни

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні роботи згідно з розкладом, не запізнюватися на заняття, домашні завдання виконувати відповідно до графіка. Пропущене практичне заняття студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До лабораторних робіт студент має підготуватися за відповідною темою і проявляти активність. При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-poryadok-vyznannya-ta-perezarahuvannya-rezultativ-navchannya.pdf.

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. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

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	Т 2-3	Залік
ВК:	0,8	0,2	0,2	

Оцінювання лабораторних робіт. 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 он-лайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал 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.

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.

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. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
9. The Basics of Digital Forensics The Primer for Getting Started in Digital Forensics. Second Edition / John Sammons. – Elsevier Inc., 2015. – 180 p.
10. Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с.
11. 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.
12. 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.
13. 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.
14. 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

15. 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.
16. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
17. Поняття та класифікація віртуальних слідів кіберзлочинів // Я. Найдьон. / Криміналістика. – 2019. – №5. – С. 304-307.
18. 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.
19. 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.
20. 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.
21. Шеломенцев В. П. Віртуальність як елемент характеристики кіберзлочинів. Часопис Національного університету "Острозька академія". Серія "Право". – 2011. – №1(3). – С. 1-15

22. 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.
23. Гладун А.Я. Таксономія стандартів інформаційної безпеки / А.Я. Гладун, К.О. Хала // Наука, технології, інновації. – 2017. – № 2. – С. 53-64
24. 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.
25. 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.
26. 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.
27. 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.
28. Борсуковський Ю. В. Визначення сучасних вимог до створення політики управління доступом корпоративних користувачів / Ю. В. Борсуковський // Сучасний захист інформації. – 2016. – № 4. – С. 5-9.
29. 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.
30. Ахрамович В. М. Адміністративний рівень інформаційної безпеки / В. М. Ахрамович // Сучасний захист інформації. – 2017. – № 1. – С. 10-14.
31. 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.
32. 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.
33. 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.
34. 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.
35. 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.
36. 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.
37. 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.
38. 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.
39. Hemdan, E.ED., Manjaiah, D. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimed Tools Appl 80, 14255–14282 (2021).
40. 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/.