МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності факультету №4

РОБОЧА ПРОГРАМА

навчальної дисципліни "Цифрова криміналістика"
обов'язкових компонент
освітньої програми першого рівня вищої освіти

"Кібербезпека (безпека інформаційних та комунікаційних систем)"

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол №7 від 30.08.2023

СХВАЛЕНО
Вченою радою факультету №4
Протокол № 8 від 16.08.2023

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол №7 від 29.08.2023

Розглянуто на засіданні кафедри протидії кіберзлочинності (протокол № 19 від 15.08.2023)

Розробник: професор кафедри протидії кіберзлочинності ХНУВС, к.т.н. доцент Носов В.В.

Рецензенти:

доцент кафедри кібербезпеки та DATA-технологій факультету №6 Харківського національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, д.т.н. професор Петров К.Е.

1. Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Кількість кредитів ECTS – 8
Загальна кількість годин – 240
Кількість тем – 14</td><td>12 Інформаційні технології
125 Кібербезпека (Поліцейські)
бакалавр</td><td>Навчальний курс 4
Семестри 7, 8
Види підсумкового контролю:
- залік у семестрі 7.
- екзамен у семестрі 8.</td></tr>
<tr><td colspan="3">Розподіл навчальної дисципліни за видами занять:</td></tr>
<tr><td colspan="2">денна форма навчання
Семестр 7:
Лекції – 20 год;
Лабораторні заняття - 40 год;
Самостійна робота – 60 год;

Індивідуальні завдання:
Реферати (тощо) – 1

Семестр 8:
Лекції – 20 год;
Лабораторні заняття - 40 год;
Самостійна робота – 60 год;

Індивідуальні завдання:
Реферати (тощо) – 1</td><td>заочна форма навчання
Семестр 7:
Лекції – 20 год;
Лабораторні заняття - 40 год;
Самостійна робота – 60 год;

Індивідуальні завдання:
Реферати (тощо) – 1

Семестр 8:
Лекції – 20 год;
Лабораторні заняття - 40 год;
Самостійна робота – 60 год;

Індивідуальні завдання:
Реферати (тощо) – 1</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Мета: формування знань і вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки.

Завдання:

• отримання знань щодо криміналістичних досліджень сучасних інформаційних систем і носіїв даних;

• формування вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки.

Міждисциплінарні зв'язки: спирається на Основи кібербезпеки, Теорію інформації та кодування; Операційні системи та комп'ютерні мережі, Безпека інформаційно-комунікаційних систем.

Очікувані результати навчання:

знати: поняття електронних (цифрових) доказів, процедури первинних цифрових криміналістичних досліджень, структуру жорсткого диску та файлових систем, методи та засоби вилучення даних та створення дублікатів носіїв даних, методи протидії криміналістичним дослідженням;

вміти проводити криміналістичні дослідження: операційних систем, комп'ютерних мереж, веб-атак, баз даних, хмарних сервісів, шкідливого програмного забезпечення, електронної пошти, мобільних пристроїв.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.	
Загальні компетентності (ЗК)	ЗК 1	Здатність застосовувати знання у практичних ситуаціях.
	ЗК 2	Знання та розуміння предметної області та розуміння професії.
	ЗК 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
	ЗК 5	Здатність до пошуку, оброблення та аналізу інформації
Фахові компетентності спеціальності (ФК)	ФК 1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
	ФК 8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

3. Програма навчальної дисципліни

Тема № 1. Електронні (цифрові) докази

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

Тема № 2. Процес первинних цифрових криміналістичних досліджень

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

Тема № 3. Структура жорсткого диску та файлових систем

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

Тема № 4. Здобуття даних та створення дублікатів носіїв даних

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

Тема № 5. Подолання протидії криміналістичним дослідженням

Поняття протидії криміналістичним дослідженням. Методи протидії криміналістичним дослідженням. Отримання доказів з видалених файлів і розділів, зашифрованих файлів, стеганографічних об'єктів. Ідентифікація обфускації, витирання залишків, перезапису даних та метаданих, шифрування. Криптографічні мережні протоколи, програмні пакувальники, руткіти як методи протидії криміналістичним дослідженням. Контрзаходи протидії криміналістичним дослідженням. Основні виклики у подоланні протидії криміналістичним дослідженням.

Тема № 6. Криміналістичні дослідження операційних систем

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

Тема № 7. Криміналістичні дослідження комп'ютерних мереж

Сутність криміналістичного дослідження комп'ютерних мереж. Протоколювання трафіку комп'ютерної мережі. Принципи взаємозв'язків подій. Підготовка і етапи проведення криміналістичного дослідження комп'ютерних мереж. Огляд

маршрутизатору, міжмережного екрану, системи виявлення вторгнень, DHCP-сервера, баз даних. Огляд трафіку. Документування отриманих із мережі доказів. Реконструкція доказів.

Тема № 8. Криміналістичні дослідження веб-атак

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

Тема № 9. Криміналістичні дослідження баз даних

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

Тема № 10. Криміналістичні дослідження хмарних сервісів

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

Тема № 11. Криміналістичні дослідження шкідливого програмного забезпечення

Шкідливе програмне забезпечення (ШПЗ) та шляхи його впровадження в систему. Методи розповсюдження ШПЗ. Основні складові ШПЗ. Принципи криміналістичного дослідження ШПЗ. Ідентифікація і вилучення ШПЗ з включеної і виключеної системи. Створення лабораторії і середовища з аналізу шкідливих програм. Правила лабораторного аналізу ШПЗ. Динамічний і статичний аналіз. Виклики, що виникають під час проведення криміналістичного дослідження ШПЗ.

Тема № 12. Криміналістичні дослідження електронної пошти

Архітектура системи електронної пошти, сервери і клієнти, їх характеристики. Важливість електронних повідомлень. Злочини, де використовується електронна пошта. Складові листа електронної пошти, службові заголовки листа. Етапи криміналістичного дослідження електронних листів зловмисників і потерпілих. Інструменти криміналістичного дослідження електронної пошти.

Тема № 13. Криміналістичні дослідження мобільних пристроїв

Необхідність криміналістичного дослідження мобільних пристроїв. Роль апаратних і програмних платформ у криміналістичного дослідження мобільних пристроїв. Рівні архітектури оточення мобільних пристроїв. Стек архітектури Android і процеси завантаження системи. Стек архітектури iOS і процеси завантаження системи. Визначення місць збереження доказових даних. Підготовка до криміналістичного дослідження мобільних пристроїв. Криміналістичні дослідження мобільних пристроїв.

Тема № 14. Складання звіту і представлення результатів криміналістичних досліджень

Важливість оформлення звіту щодо результатів криміналістичних досліджень. Узагальнений шаблон звіту криміналістичних досліджень. Види звітів та методика їх складання. Спеціаліст з первинних криміналістичних досліджень як свідок. Порівняння ролей експертів і технічних спеціалістів. Свідчення спеціаліста у суді.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни				Вид контролю
	Всього	з них:			
		Лекції	Лабораторні заняття	Самостійна робота	
Семестр №7					
Тема № 1. Електронні (цифрові) докази	4	2		2	**залік**
Тема № 2. Процес первинних цифрових криміналістичних досліджень	20	4	6	10	
Тема № 3. Структура жорсткого диску та файлових систем	20	4	6	10	
Тема № 4. Вилучення даних та створення дублікатів носіїв даних	24	2	10	12	
Тема № 5. Методи протидії криміналістичним дослідженням	20	4	6	10	
Тема № 6. Криміналістичні дослідження операційних систем	32	4	12	16	
Всього за семестр №7	**120**	**20**	**40**	**60**	
Семестр №8					
Тема № 7. Криміналістичні дослідження комп'ютерних мереж	20	4	6	10	**екзамен**
Тема № 8. Криміналістичні дослідження веб-атак	16	2	6	8	
Тема № 9. Криміналістичні дослідження баз даних	16	2	6	8	
Тема № 10. Криміналістичні дослідження хмарних сервісів	16	2	6	8	
Тема № 11. Криміналістичні дослідження шкідливого програмного забезпечення	16	2	6	8	
Тема № 12. Криміналістичні дослідження електронної пошти	12	2	4	6	
Тема № 13. Криміналістичні дослідження мобільних пристроїв	20	4	6	10	
Тема № 14. Складання звіту і представлення результатів криміналістичних досліджень	4	2		2	
Всього за семестр №8	**120**	**20**	**40**	**60**	
Всього за дисципліною	**240**	**40**	**80**	**120**	

4.1.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни				Вид контролю
	Всього	з них:			
		Лекції	Лабораторні заняття	Самостійна робота	
Семестр №7					
Тема № 1. Електронні (цифрові) докази	4	1	1	2	**залік**
Тема № 2. Процес первинних цифрових криміналістичних досліджень	20	1	1	18	
Тема № 3. Структура жорсткого диску та файлових систем	20	1	1	18	
Тема № 4. Вилучення даних та створення дублікатів носіїв даних	24	1	1	22	
Тема № 5. Методи протидії криміналістичним дослідженням	20	1	1	18	
Тема № 6. Криміналістичні дослідження операційних систем	32	1	1	30	
Всього за семестр №7	**120**	**6**	**6**	**108**	
Семестр №8					
Тема № 7. Криміналістичні дослідження комп'ютерних мереж	20	1	1	18	**екзамен**
Тема № 8. Криміналістичні дослідження веб-атак	16	1	1	14	
Тема № 9. Криміналістичні дослідження баз даних	16	1		15	
Тема № 10. Криміналістичні дослідження хмарних сервісів	16	1	1	14	
Тема № 11. Криміналістичні дослідження шкідливого програмного забезпечення	16	1	1	14	
Тема № 12. Криміналістичні дослідження електронної пошти	12	1		11	
Тема № 13. Криміналістичні дослідження мобільних пристроїв	20		1	19	
Тема № 14. Складання звіту і представлення результатів криміналістичних досліджень	4		1	3	
Всього за семестр №8	**120**	**6**	**6**	**108**	
Всього за дисципліною	**240**	**8**	**16**	**216**	

4.1.2. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література
Тема №1. Електронні (цифрові) докази	
1. Визначення електронних доказів в правовому полі України. 2. Визначення електронних доказів в ЄС. 3. Визначення електронних доказів в США.	Ресурси Internet
Тема №2. Процес первинних цифрових криміналістичних досліджень	
1. Склад апаратних та open source програмних засобів первинних цифрових криміналістичних досліджень. 2. Порядок передачі та зберігання (chain of custody) електронних доказів	Ресурси Internet
Тема №3. Структура жорсткого диску та файлових систем	
1. Файлові системи ОС Windows. 2. Файлові системи ОС Linux. 3. Файлові системи ОС Mac.	Ресурси Internet
Тема №4. Вилучення даних та створення дублікатів носіїв даних	
1. Послідовність у вилученні та дублюванні даних. 2. Найкращі практики вилучення даних.	Ресурси Internet
Тема №5. Подолання протидії криміналістичним дослідженням	
1. Контрзаходи протидії криміналістичним дослідженням. 2. Основні виклики у подоланні протидії криміналістичним дослідженням.	Ресурси Internet
Тема №6. Криміналістичні дослідження операційних систем	
1. Аналіз журналів подій Linux. Збір і огляд енергонезалежних і енергозалежнихданих з Linux комп'ютерів. 2. Аналіз файлів і журналів подій Mac комп'ютерів.	Ресурси Internet
Тема №7. Криміналістичні дослідження комп'ютерних мереж	
1. Документування отриманих з мережі доказів. 2. Реконструкція доказів.	Ресурси Internet
Тема №8. Криміналістичні дослідження веб-атак	
1. Архітектура Apache веб-сервера і криміналістичний аналіз його лог-файлів. 2. Розслідування різноманітних атак на веб-застосунки.	Ресурси Internet
Тема №9. Криміналістичні дослідження баз даних	
1. Інструменти криміналістичного дослідження MySQL. 2. Криміналістичне дослідження MySQL на WordPress.	Ресурси Internet
Тема №10. Криміналістичні дослідження хмарних сервісів	
1. Виклики, що виникають під час проведення криміналістичного дослідження хмарних сервісів. 2. Криміналістичне дослідження хмарних сховищ Dropbox та Google Drive.	Ресурси Internet
Тема №11. Криміналістичні дослідження шкідливого програмного забезпечення	
1. Динамічний і статичний аналіз. 2. Виклики, що виникають під час проведення криміналістичного дослідження ШПЗ.	Ресурси Internet
Тема №12. Криміналістичні дослідження електронної пошти	
1. Етапи криміналістичного дослідження електронних листів зловмисників і потерпілих. 2. Інструменти криміналістичного дослідження електронної пошти.	Ресурси Internet
Тема № 13. Криміналістичні дослідження мобільних пристроїв	

	Перелік питань до тем навчальної дисципліни	Література
	1. Підготовка до криміналістичного дослідження мобільних пристроїв. 2. Криміналістичні дослідження мобільних пристроїв.	Ресурси Internet
	Тема № 14. Складання звіту і представлення результатів криміналістичних досліджень	
	1. Порівняння ролей експертів і технічних спеціалістів. 2. Свідчення спеціаліста у суді.	Ресурси Internet

5. Індивідуальні навчально-дослідні завдання

5.1.1. Теми рефератів

1. Computer Forensics Tool Testing Program.
2. National Software Reference Library.
3. Digital Forensics and Incident Response Cheat Sheets and Posters.
4. Automatic profile generation for live Linux Memory analysis.
5. Free Tool Magnet Forensics.
6. Computer Aided INvestigative Environment.
7. Sysinternals Suite.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких курсанти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань практичних і лабораторних занять.

Індивідуальна робота передбачає написання рефератів.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

Контроль проводиться по тестових завданнях на підсумковому контролі – заліку та екзамені.

Екзаменаційні тестові питання

1. На якому етапі роботи з цифровими доказами здійснюється фіксація цифрових слідів?
2. Яка інформація відноситься до летючих даних (volatile data)?
3. Що не відноситься до об'єктів криміналістичного аналізу в ОС Windows?
4. Де не має летючих даних (volatile data)?
5. Як фіксується стан цифрових слідів?
6. В якому файлі НЕ зберігаються журнали аудиту подій ОС (Windows Event Logs)?
7. Чи фіксується у журналі аудиту Windows зміна політики аудиту?
8. Де зберігається локальна облікова інформація про паролі користувачів Windows?
9. Де зберігається база даних облікової інформації Active Directory Windows?
10. Яку хеш функцію використовує Windows 7 для збереження паролів облікових записів?

11. Яку хеш функцію використовує Windows 95 для збереження паролів облікових записів?
12. Який протокол автентифікації НЕ використовує Windows для доступу до ресурсів віддалених комп'ютерів?
13. Який засіб може бути використаний для криміналістичного аналізу журналів подій Windows?
14. Від чого залежить ефективність пошуку текстової інформації в образі диску засобами криміналістичного дослідження?
15. Яка часова мітка файлу у системі FAT змінюються при його переміщенні?
16. Яка часова мітка файлу у системі FAT змінюються при його копіюванні?
17. За якою часовою міткою визначається час копіювання файлу у системі FAT?
18. За якою ознакою встановлюється факт того, що файл у системі FAT був скопійований, а не створений?
19. Які часові мітки файлу NTFS змінюються при його копіюванні?
20. За якою ознакою встановлюється факт того, що файл NTFS був скопійований?
21. Яка часова мітка каталогу NTFS змінюється при створенні та видаленні файлів каталогу?
22. Яка часова мітка каталогу NTFS змінюється при його копіюванні?
23. Що у Windows, як правило, допомагає визначити користувача, від імені якого відбулося останнє завантаження системи?
24. Що у Windows допомагає визначити момент зміни дати та часу системи?
25. До якого типу відноситься збір даних із невикористаних місць кластерів диску (slack space) у процесі комп'ютерного криміналістичного дослідження?
26. До якого типу відноситься збір даних із незайнятого (unallocated) простору диска у процесі комп'ютерного криміналістичного дослідження?
27. До якого типу відноситься збір даних із оптичних носіїв у процесі комп'ютерного криміналістичного дослідження?
28. До якого типу відноситься збір даних із системного реєстру Windows у процесі комп'ютерного криміналістичного дослідження?
29. До якого типу відноситься збір даних із кешу Windows у процесі комп'ютерного криміналістичного дослідження?
30. До якого типу відноситься збір даних із оперативній пам'яті у процесі комп'ютерного криміналістичного дослідження?
31. Який тип системи за підключенням використовується для швидкого збору даних (Data Acquisition Systems) при комп'ютерному криміналістичному дослідженні?
32. Який формат збирання даних (Data Acquisition Format) є відкритим і найбільш функціональним при комп'ютерному криміналістичному дослідженні?
33. Який метод дублювання даних використовується при комп'ютерному криміналістичному дослідженні?
34. Яким чином запобігають невимушеній модифікації оригінальних доказів у ході комп'ютерної експертизи?
35. При обмеженому часі комп'ютерного криміналістичного дослідження і дуже великому вихідному диску який метод збору даних (acquisition data copy method) як правило використовується?
36. Яка процедура забезпечує гарантії відсутності залишкових даних на цільовому носії перед дублюванням інформації з вихідного носія?
37. Що не впливає на визначення найкращого методу збору даних (дублювання)?

38. Що є неправильним при створенні криміналістичного образу диску?
39. Для якого цільового носія перед дублюванням інформації з вихідного носія не має сенсу обчислювати хеш значення?
40. Що є основним недоліком при криміналістичному зборі летючих (volatility) даних комп'ютерної системи?
41. Згідно типового алгоритму огляду комп'ютера що потрібно зробити при виявленні процесу передачі даних із віддаленим ресурсом мережі?
42. Згідно типового алгоритму огляду комп'ютера що потрібно зробити при виявлені шифрування?
43. Згідно типового алгоритму огляду комп'ютера що потрібно зробити, якщо він виявиться сервером?
44. Згідно типового алгоритму огляду комп'ютера що потрібно зробити, якщо він підключений до мережі?
45. Згідно типового алгоритму огляду комп'ютера що потрібно зробити, якщо він НЕ підключений до мережі?
46. Згідно типового алгоритму огляду комп'ютера що потрібно зробити, якщо він НЕ увімкнений?
47. Для чого потрібно обчислити хеш-значення еталонного файлу при огляді стандартних засобів комп'ютерної техніки?
48. Що таке "стерилізація" відносно носія даних?
49. Що використовується для криміналістичного аналізу файлів зображень?
50. Якою є основна вимога до процедури зняття образу оперативної пам'яті?
51. Що НЕ відбувається при видалені файлу в ОС Windows?
52. В якому випадку неможливо відновити видалені у Windows файли?
53. Де зберігається видалені файли файлової системи FAT?
54. Де зберігається повний шлях до видаленого файлу?
55. За якою маскою перейменовуються видалені файли у кошику Windows 7?
56. За якою маскою перейменовуються видалені файли у кошику Windows 98?
57. Як відновити без використання спеціальних утиліт видалений файл INFO ОС Windows?
58. Як відновити без використання спеціальних утиліт пошкоджений каталог Кошику ОС Windows?
59. Який процес відбувається із файлом у MAC OS X при його звичайному видаленні?
60. Який процес відбувається із файлом у Linux при його звичайному видаленні?
61. Як впливає видалення логічних розділів (partition) на функціональність ОС Windows?
62. Скільки існує методів відновлення файлів в Mac OS X 10.S "Leopard" при їх звичайному видаленні?
63. Скількома методами можна відновити видалені логічні розділи?
64. Що НЕ може безпосередньо виявити криміналістичне дослідження комп'ютерної мережі?
65. Які типи систем виявлення вторгнень не застосовуються у комп'ютерній мережі?
66. Яка категорія криміналістичного огляду журналів подій (logs) дає найбільші можливості розкриття злочину?

67. Що збільшує довіру до інформації, отриманої при криміналістичному аналізі журналів подій (logs)?
68. Що не забезпечує автентичність журналів подій?
69. Що НЕ використовуються для криміналістичного дослідження мережевого трафіку?
70. Що НЕ використовується для збору трафіку мережі через DNS інтоксикацію?
71. Як НЕ документується ARP таблиця?
72. Який об'єкт додається до журналу аудиту при атаці типу "Separator Injection"?
73. Який об'єкт додається до журналу аудиту при атаці типу "Word Wrap Abuse"?
74. Який об'єкт додається до журналу аудиту при атаці типу "New Line Injection"?
75. Який об'єкт додається до журналу аудиту при атаці типу "Timestamp Injection"?
76. Який об'єкт додається до журналу аудиту при атаці типу "HTML Injection"?
77. В якому випадку файли журналів аудиту не можуть розглядатися в якості доказів?
78. Що може виступати документальним підтвердженням достовірності записів журналу подій?
79. Яким чином реалізується моніторинг трафіку мережі "Intranet DNS Spoofing"?
80. Яким чином реалізується моніторинг трафіку мережі "DNS Poisoning"?
81. Який застосовується механізм для управління доступом до Wi-Fi мережі?
82. Що у мережі Wi-Fi виконує роль єдиного ідентифікатора, що розділяється всіма учасниками?
83. Які безпровідні пристрої на місці події визначаються як джерела, що здійснюють атаку?
84. Які безпровідні пристрої на місці події визначаються як джерела проведення атак?
85. Що здійснюється при виявлення безпровідних підключень шляхом активного сканування?
86. Що здійснюється при виявлення безпровідних підключень шляхом пасивного сканування?
87. Що дозволяє здійснити огляд всіх бездротових пристроїв і мереж на місці події?
88. При підключенні до точки доступу мережі Wi-Fi що потрібно зробити у першу чергу?
89. Який журнал аудиту Wi-Fi точки доступу може містити інформацію щодо вторгнення у мережу?
90. Яка атака у мережі Wi-Fi направлена на порушення конфіденційності шляхом перехоплення та аналізу трафіку незахищених застосувань?
91. Яка атака у мережі Wi-Fi направлена на порушення цілісності шляхом захоплення даних і подальшим їх відтворенням із затримкою?
92. Яка атака у мережі Wi-Fi направлена на порушення цілісності шляхом модифікації даних трафіку мережі?
93. Який протокол шифрування і автентифікації у мережі Wi-Fi є найбільш безпечним?
94. Який журнал аудиту веб серверу Apache містить запити, що обробляються сервером?
95. Який журнал аудиту веб серверу Apache зберігає діагностичну інформацію і повідомлення про помилки, що виникають при обробці запитів?
96. Файл якого журналу НЕ містить сліди атак SQL ін'єкції?

97. Що є ознаками XSS атак?
98. Яка подія НЕ свідчить про веб атаку?

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних і лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти (далі – здобувач) з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середнє арифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

Загальна кількість балів (перед підсумковим контролем) =((***Результат навчальних занять за семестр*** + ***Результат самостійної роботи за семестр***) / ***2***) ****10***

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображаються у відомості обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то

науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

Підсумкові бали навчальної дисципліни = ***Загальна кількість балів (перед підсумковим контролем)*** + ***Кількість балів за підсумковим контролем***

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середнє арифметичне значення балів, набраних у поточному та попередньому семестрах.

Підсумкові бали навчальної дисципліни = ***Підсумкові бали за поточний семестр*** + ***Підсумкові бали за попередній семестр*** : ***2***

Критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на практичних, лабораторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю.

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати звіт за темою самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97–100	Відмінно ("зараховано")	A	**"Відмінно"** – теоретичний зміст курсу освоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85– 89	Добре ("зараховано")	B	**"Дуже добре"** – теоретичний зміст курсу освоєний **цілком**, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома – трьома незначними помилками.
80-84			
75–79		C	**"Добре"** – теоретичний зміст курсу освоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією – двома значними помилками.
70 –74	Задовільно ("зараховано")	D	**"Задовільно"** – теоретичний зміст курсу освоєний **не повністю**, але **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань, містять **помилки,** робота з трьома значними помилками.
65-69			
60–64		E	**"Достатньо"** – теоретичний зміст курсу освоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконані,** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
41–59	Незадовільно ("не зараховано")	FX	**"Умовно незадовільно"** – теоретичний зміст курсу освоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм навчання, навчальних завдань **не виконано**, або якість їхнього виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки
21-40			
1–20		F	**"Безумовно незадовільно"** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не сформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не призведе** до значного **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки

10. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна

1. EC-Council. Computer Hacking Forensic Investigator v9. Courseware.
2. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів.
3. Петрович Л. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України / Л. Петрович, Н. В'ятов. – К. : Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні»), 2014. – 60 с.
4. Про судову експертизу: закон України від 25.02.1994 р.; [із змінами і доповненнями на 01.04.2015] // Відомості Верховної Ради України. – 1994. – № 28 (12.07.1994). – ст. 232.
5. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Міністерства юстиції України № 53/5 від 08.10.1998 р. [із змінами і доповненнями на 22.01.2013] // Офіційний вісник України. – 1998. – № 46 (03.12.1998). – ст. 1715.
6. Стандартні робочі процедури для збирання, аналізу та демонстрації електронних доказів / Офіс програми протидії кіберзлочинності Ради Європи (C-PROC) / Електронна версія від 12 вересня 2019 року.
7. Посібник з питань електронних доказів. Базовий посібник для співробітників правоохоронних органів, прокурорів та суддів / Відділ протидії кіберзлочинності. Генеральний директорат з прав людини та верховенства права Ради Європи / Електронна версія 2.1, Страсбург, Франція, 6 березня 2020 року.
8. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. – К., 2017. – 148 с.
9. Посібник для підвищення кваліфікації працівників органів та підрозділів Національної поліції України / О.І. Безпалова, КЛ. Бугайчук, А.В. Волховський та ін. Харків, нац. ун-т внутр. справ. Харків: ХНУВС. 2019. 132 с.

Додаткова

10. Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Third Edition. Edited by Eoghan Casey. www.elsevierdirect.com/companions/9780123742681.
11. Handbook of Digital Forensics and Investigation Edited by Eoghan Casey. http://www.elsevierdirect.com/product.jsp?isbn=9780123742674.
12. Digital Forensics and Preservation. Digital Preservation Coalition and Jeremy Leighton John. [Електронний ресурс] / Published in association with Charles Beagrie Ltd. 2012. Режим доступу: http://dx.doi.org/10.7207/twr12-03.

Інформаційні ресурси

13. https://securityonline.info/category/forensics/
14. https://resources.infosecinstitute.com/category/forensics-2/
15. http://www.dfrws.org/
16. https://www.forensicmethods.com