

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра кібербезпеки та DATA – технологій факультету №6

**МЕТОДИЧНІ МАТЕРІАЛИ
ДО ЛАБОРАТОРНИХ ЗАНЯТЬ**

з навчальної дисципліни "Цифрова криміналістика"
вибіркових компонент
освітньої програми першого рівня вищої освіти

125 "Кібербезпека" (Безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30 . 08 .2023р. № 71

СХВАЛЕНО

Вченою радою факультету № 6
Протокол від 25 .08 .2023 р. № 7

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29 .08 .2023р. № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA технологій
факультету № 6
(протокол від 15 .08 .2023р. № 8)

Розробники: професор кафедри кібербезпеки та DATA – технологій ХНУВС, к.т.н.
доцент Носов В.В.;
доцент кафедри кібербезпеки та DATA – технологій ХНУВС, д.т.н. Можєєв М.О.

Рецензенти:

- 1. Доцент кафедри боротьби з кіберзлочинністю ХНУВС, к.т.н., доцент
Клімушин П.С.;*
- 2. Завідувач кафедри ЕОМ ХНУРЕ д.т.н., професор Коваленко А.А.*

1. Розподіл часу навчальної дисципліни за темами

2. Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практич	Лаборат	Самості	
Семестр №6						
Тема № 1. Електронні (цифрові) докази	14	4			10	залік
Тема № 2. Процес первинних цифрових криміналістичних досліджень	42	8	4	8	22	
Тема № 3. Структура жорсткого диску та файлових систем	34	6	6	8	14	
Всього за семестр №6	90	18	10	16	46	
Семестр №7						
Тема № 4. Вилучення даних та створення дублікатів носіїв даних	20	4	2	4	10	екзамен
Тема № 5. Методи протидії криміналістичним дослідженням	24	6	2	4	12	
Тема № 6. Криміналістичні дослідження операційних систем	30	6	4	4	16	
Тема № 7. Криміналістичні дослідження комп'ютерних мереж	28	6	4	6	12	
Тема № 8. Криміналістичні дослідження веб-атак	18	4	2	2	10	
Всього за семестр №7	120	26	14	20	60	
Семестр №8						
Тема № 9. Криміналістичні дослідження баз даних	24	6	2	4	12	екзамен
Тема № 10. Криміналістичні дослідження хмарних сервісів	20	4	2	4	10	
Тема № 11. Криміналістичні дослідження шкідливого програмного забезпечення	20	4	2	4	10	

2. Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практич	Лаборат	Самості	
Тема № 12. Криміналістичні дослідження електронної пошти	16	4	2	2	8	
Тема № 13. Криміналістичні дослідження мобільних пристроїв	28	6	4	6	12	
Тема № 14. Складання звіту і представлення результатів криміналістичних досліджень	12	4			8	
Всього за семестр №8	120	28	12	20	60	
Всього за дисципліною	330	72	36	56	166	

2. Методичні вказівки до лабораторних занять Семестр №6

Тема № 2. Процес первинних цифрових криміналістичних досліджень
Лабораторне заняття 2.1. Відновлення видалених файлів і логічних розділів носіїв даних

Навчальна мета заняття: отримати навик використання засобів з відновлення видалених даних, навчитися застосовувати ефективні інструменти при різних задачах.

Кількість годин: 4 год.

Навчальні питання

1. Відновлення даних
2. Порівняльний аналіз ефективності засобів відновлення видалених даних

Література:

1. Матеріали лекції і керівництва до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 2.2. Засоби огляду файлів різних форматів

Навчальна мета заняття: отримати навички використання засобів огляду файлів різних форматів.

Кількість годин: 2 год.

Навчальні питання

1. File Viewer
2. File Viewer Lite

Література:

1. Матеріали за темою 2 і керівництва до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Засоби, які можуть бути використані в роботі:

- File Viewer;
- File Viewer Lite

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 2.3. Криміналістичне відновлення видалених і пошкоджених файлів в ОС Linux

Навчальна мета заняття: отримати навички відновлення видалених і пошкоджених файлів в ОС Linux.

Кількість годин: 2 год.

Навчальні питання

1. Foremost
2. Magicrescue

Література:

1. Матеріали за темою 2 і керівництва до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Засоби, які можуть бути використані в роботі:

- Foremost
- Magicrescue

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №3. Структура жорсткого диску та файлових систем

Лабораторне заняття 3.1. Аналіз образу жорсткого диску за допомогою AutoPsy

Навчальна мета заняття: отримати навички аналізу образу жорсткого диску

Кількість годин: 4 год.

Навчальні питання

1. Встановлення та налаштування AutoPsy
2. Аналіз образу жорсткого диску за допомогою AutoPsy

Література:

1. Матеріали за темою 3 і керівництво до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Семестр №7

Тема №4. Вилучення даних та створення дублікатів носіїв даних

Лабораторне заняття 4.1. Вивчення інструментів збору даних та створення дублікатів носіїв даних спеціалізованих Linux систем

Навчальна мета заняття: отримати навички створення дублікатів носіїв даних.

Кількість годин: 4 год.

Навчальні питання

1. Створення Live Pendrive Caine 10.0.
2. Вивчення інструментів збору даних та створення дублікатів носіїв у Caine 10.0.
3. Вивчення інструментів збору даних та створення дублікатів носіїв у Kali Linux.

Література:

1. Матеріали за темою 4 і керівництво до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №5. Подолання протидії криміналістичним дослідженням

Лабораторне заняття 5.1. Подолання протидії криміналістичним дослідженням

Навчальна мета заняття: отримати навички виявлення електронних доказів, що приховані від дослідження

Кількість годин: 4 год.

Навчальні питання

1. НА: Forensics.

Література:

1. Матеріали за темою 5 і керівництво до лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №6. Криміналістичні дослідження операційних систем Лабораторне заняття 6.1. Здобуття та аналіз реєстру ОС Windows

Навчальна мета заняття: навчитися користуватися засобами криміналістичного здобуття та аналізу реєстру ОС Windows.

Кількість годин: 4 год.

Навчальні питання

1. Встановлення та ознайомлення із RegRipper.
2. Здобуття та аналіз реєстру ОС Windows.

Література:

1. Керівництво до практичних і лабораторних занять.
2. <https://www.hackingarticles.in/forensic-investigation-windows-registry-analysis/>

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 6.2. Здобуття нестійких даних з ОС Linux

Навчальна мета заняття: ознайомитися із засобами криміналістичного дослідження ОС Linux.

Кількість годин: 4 год.

Навчальні питання

1. Вилучення енергетично залежних даних в ОС Linux.
2. Вилучення енергетично незалежних даних в ОС Linux.

Література:

1. Керівництво до практичних і лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №7. Криміналістичні дослідження комп'ютерних мереж

Лабораторне заняття 7.2. Криміналістичне дослідження журналів аудиту мережних подій

Навчальна мета заняття: навчитися користуватися засобами криміналістичного дослідження журналів аудиту мережних подій.

Кількість годин: 4 год.

Навчальні питання

1. Застосування засобу Xpolog Center Suite.
2. Застосування засобу Kiwi Log Viewer.

Література:

1. Керівництво до практичних і лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 8.1. Криміналістичне дослідження мережного трафіку

Навчальна мета заняття: ознайомитися із засобами криміналістичного дослідження ОС Linux.

Кількість годин: 2 год.

Навчальні питання

1. Встановлення і налаштування Wireshark.
2. Розв'язання практичних завдань.

Література:

1. Керівництво до практичних і лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №8. Криміналістичні дослідження веб-атак

Лабораторне заняття 10. Розслідування веб-атак

Навчальна мета заняття: ознайомитися із прикладом розслідування веб-атак.

Кількість годин: 2 год.

Навчальні питання

1. Визначення питань розслідування.
2. Виконання розслідування.

Література:

1. Керівництво до практичних і лабораторних занять.
2. <http://honeynet.org/challenges>.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Семестр №8

Тема №9. Криміналістичні дослідження баз даних

Лабораторне заняття 11. Криміналістичні дослідження MySQL Server Database

Навчальна мета заняття: отримати навички криміналістичного дослідження MySQL Server Database.

Кількість годин: 4 год.

Навчальні питання

1. Встановлення і налаштування WampServer.
2. Виконання дослідження MySQL Server Database за допомогою Hex Workshop Hex Editor.

Література:

1. Керівництво до практичних і лабораторних занять.
2. <http://honeynet.org/challenges>.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №10. Криміналістичні дослідження хмарних сервісів

Лабораторне заняття 12. Криміналістичні дослідження хмарних сховищ

Навчальна мета заняття: отримати навички криміналістичного дослідження хмарних сховищ Dropbox і Google Drive.

Кількість годин: 4 год.

Навчальні питання

1. Дослідження хмарного сховища Dropbox.
2. Дослідження хмарного сховища Google Drive.

Література:

1. Керівництво до практичних і лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №11. Криміналістичні дослідження шкідливого програмного забезпечення Лабораторне заняття 13. Статичний і динамічний аналіз шкідливого програмного забезпечення

Навчальна мета заняття: отримати навички статичного і динамічного аналізу шкідливого програмного забезпечення.

Кількість годин: 4 год.

Навчальні питання

1. Статичний аналіз підозрілих файлів.
2. Динамічний аналіз шкідливого програмного забезпечення.

Література:

1. Керівництво до практичних і лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №12. Криміналістичні дослідження електронної пошти

Лабораторне заняття 14. Криміналістичні дослідження скриньок електронної пошти

Навчальна мета заняття: отримати навички криміналістичного дослідження скриньок електронної пошти.

Кількість годин: 2 год.

Навчальні питання

1. Відновлення видалених електронних листів утилітою Recover My Email.
2. Криміналістичне дослідження скриньки електронної пошти утилітою Paraben's Email Examiner.

Література:

1. Керівництво до практичних і лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №13. Криміналістичні дослідження мобільних пристроїв

Лабораторне заняття 15. Криміналістичні дослідження образу Android терміналу

Навчальна мета заняття: отримати навички криміналістичного дослідження образу Android терміналу.

Кількість годин: 6 год.

Навчальні питання

1. Дослідження образу Android терміналу за допомогою Autopsy.
2. Дослідження образу Android терміналу за допомогою Andriller.

Література:

1. Керівництво до практичних і лабораторних занять.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Криміналістика: Підручник / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. — 4-е вид., перероб. і доп. — Х.: Право, 2012. — 464 с.
2. EC-Council. Computer Hacking Forensic Investigator v9. Courseware.
3. ДСТУ ISO/IEC 27037:2017. Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжєвський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. — К., 2017. — 148 с.

- 10.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.
- 11.**Допоміжна**
- 12.Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Third Edition. Edited by Eoghan Casey. www.elsevierdirect.com/companions/9780123742681.
- 13.Handbook of Digital Forensics and Investigation Edited by Eoghan Casey. <http://www.elsevierdirect.com/product.jsp?isbn=9780123742674>.
- 14.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>.
- 15.**Інформаційні ресурси**
- 16.<https://securityonline.info/category/forensics/>
- 17.<https://resources.infosecinstitute.com/category/forensics-2/>
- 18.<http://www.dfrws.org/>
- 19.<https://www.forensicmethods.com>