

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

Кафедра протидії кіберзлочинності факультету №4

**МЕТОДИЧНІ МАТЕРІАЛИ
ДО ЛАБОРАТОРНИХ ЗАНЯТЬ**

з 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. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни				Вид контр
	Всього	з них:			
		лекції	Лаб. зан.	Сам. роб.	
Семестр №7					
Тема № 1. Електронні (цифрові) докази	4	2		2	залік
Тема № 2. Процес первинних цифрових криміналістичних досліджень	28	4	10	14	
Тема № 3. Структура жорсткого диску та файлових систем	20	4	6	10	
Тема № 4. Вилучення даних та створення дублікатів носіїв даних	16	2	6	8	
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	екза мен
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	

2. Методичні вказівки до лабораторних занять

Семестр №7

Тема № 2. Процес первинних цифрових криміналістичних досліджень

Лабораторне заняття 2.1. Апаратні і програмні засоби цифрової криміналістики

Навчальна мета заняття: ознайомитись із актуальними апаратними і програмними засобами цифрової криміналістики

Кількість годин: 2 год.

Навчальні питання

Вступ

1. Апаратні засоби цифрової криміналістики
2. Програмні засоби цифрової криміналістики

Висновки

Література:

1. Матеріали за темою 2.
2. [2].

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 лабораторних занять за темою виконують задачі навчальних питань.

Задача 1. Класифікувати і визначити призначення апаратних засобів цифрової криміналістики.

Задача 2. Класифікувати і визначити призначення програмних засобів цифрової криміналістики.

Додаткова задача для самостійної роботи:

Задача 3*. Побудувати асоціативну карту (mind map tools) апаратних і програмних засобів цифрової криміналістики за зразком <https://www.amanhardikar.com/mindmaps/Forensics.html>.

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. Обчислення криптографічних дайджестів

Навчальна мета заняття: засвоїти принцип роботи із програмними засобами обчислення криптографічних дайджестів

Кількість годин: 2 год.

Навчальні питання

1. Засоби обчислення криптографічних дайджестів
2. Порівняльний аналіз засобів обчислення криптографічних дайджестів

Література:

1. Матеріали за темою 2.
2. [2].

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 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 2.3. 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: 2 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 2.4. 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 проєктору.

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. Відновлення видалених файлів утилітою WinHex

Навчальна мета заняття: ознайомитися із функціональністю утиліти WinHex щодо відновлення видалених файлів

Кількість годин: 2 год.

Навчальні питання

1. Відновлення даних з жорсткого диску за допомогою WinHex

Література:

1. Матеріали за темою 2.
2. [2].

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

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 проєктору.

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 3.2. Встановлення форматів файлів з пошкодженими розширеннями

Навчальна мета заняття: отримати навички встановлення форматів файлів з пошкодженими розширеннями

Кількість годин: 2 год.

Навчальні питання

1. Сигнатури перших байт для різних типів файлів
2. Встановлення форматів файлів з пошкодженими розширеннями

Література:

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

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

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 проєктору.

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 3.3. Отримання метаданих файлів з пошкодженими розширеннями

Навчальна мета заняття: отримати навички аналізу метаданих файлів з пошкодженими розширеннями

Кількість годин: 2 год.

Навчальні питання

1. Встановлення та знайомство з ExifTool
2. Отримання метаданих файлів з пошкодженими розширеннями

Література:

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

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

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 проєктору.

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 №4. Вилучення даних та створення дублікатів носіїв даних

Лабораторне заняття 4.1. Стерилізація носіїв даних

Навчальна мета заняття: ознайомитись із засобами стерилізації носіїв даних

Кількість годин: 2 год.

Навчальні питання

1. Стерилізація в ОС Windows
2. Стерилізація в ОС Linux

Література:

1. Матеріали за темою 4.
2. [2].

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 4.2. Засоби здобуття 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 11.0.
2. Засоби здобуття даних та створення дублікатів носіїв у Caine 11.0.
3. Засоби здобуття 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.

Лабораторне заняття 4.3. Засоби здобуття образу RAM

Навчальна мета заняття: отримати навички здобуття образу RAM.

Кількість годин: 2 год.

Навчальні питання

1. Здобуття Windows RAM.

2. Здобуття Linux RAM.

Література:

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

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

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 проєктору.

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 4.4. Здобуття нестійких даних в Windows системах

Навчальна мета заняття: отримати навички здобуття нестійких даних в Windows системах.

Кількість годин: 2 год.

Навчальні питання

1. Огляд засобів здобуття нестійких даних в Windows системах.
2. Застосування засобів здобуття нестійких даних в Windows системах.

Література:

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

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

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 проєктору.

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 проєктор.

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 проєктору.

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 5.2. Виявлення стеганографічних об'єктів

Навчальна мета заняття: отримати навички виявлення електронних доказів, що приховані за допомогою стеганографії

Кількість годин: 2 год.

Навчальні питання

2. Створення стеганографічних контейнерів.
3. Виявлення прихованих даних утилітою StegSpy.
4. Виявлення прихованих даних утилітою OpenStego.

Література:

1. Матеріали за темою 5.
2. [2].

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

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 проєктору.

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. Аналіз RAM образу

Навчальна мета заняття: навчитися аналізувати RAM образ

Кількість годин: 4 год.

Навчальні питання

1. Встановлення та ознайомлення із Volatility.
2. Аналіз образу оперативної пам'яті

Література:

1. Матеріали за темою 6.
2. [2].

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 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 6.3. 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 проєктор.

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 проєктору.

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 №7. Криміналістичні дослідження комп'ютерних мереж

Лабораторне заняття 7.1. Застосування Wireshark для криміналістичного дослідження мережного трафіку

Навчальна мета заняття: ознайомитися із засобом Wireshark для криміналістичного дослідження трафіку.

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 проєктор.

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 проєктору.

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 7.2. Криміналістичне дослідження трафіку «Hack the Box – MarketDump»

Навчальна мета заняття: навчитися користуватися засобами криміналістичного дослідження трафіку.

Кількість годин: 2 год.

Навчальні питання

1. Постановка задачі «Hack the Box – MarketDump».
2. Знаходження прапору CTF.

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 7.3. Криміналістичне дослідження трафіку «Hack the Box – Marshal in the Middle»

Навчальна мета заняття: навчитися користуватися засобами криміналістичного дослідження трафіку.

Кількість годин: 2 год.

Навчальні питання

3. Постановка задачі «Hack the Box – Marshal in the Middle».
4. Знаходження прапору CTF.

Література:

2. 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 8.1. Аналіз доменів і IP адрес

Навчальна мета заняття: ознайомитись із засобом аналізу доменів і IP адрес.

Кількість годин: 2 год.

Навчальні питання

1. Встановлення і налаштування SmartWhois
2. Виконання практичних завдань

Література:

1. Матеріали за темою 8.
2. [2].

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 8.2. Розслідування веб-атак

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

Кількість годин: 4 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.

Тема №9. Криміналістичні дослідження баз даних

Лабораторне заняття 9.1. Засоби криміналістичного дослідження баз даних

Навчальна мета заняття: ознайомитися із засобами криміналістичного дослідження баз даних

Кількість годин: 2 год.

Навчальні питання

1. Вилучення баз даних з емулятора Android утилітою Andriller
2. Аналіз SQLite Databases утилітою DB Browser for SQLite

Література:

1. Керівництво до практичних і лабораторних занять

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

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 проєктору.

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 9.2. 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 проєктор.

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 проєктору.

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 10.1. Клієнти хмарних сховищ

Навчальна мета заняття: ознайомитись із особливостями функціонування клієнтів хмарних сховищ.

Кількість годин: 2 год.

Навчальні питання

1. Встановлення і налаштування клієнта Dropbox
2. Встановлення і налаштування клієнта Google Drive
3. Встановлення і налаштування клієнта Mega

Література:

1. Матеріали темою 10.
2. [2].

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 10.2. 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 проєктору.

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 11.1. Статичний і динамічний аналіз шкідливих програм**

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

Кількість годин: 6 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 проєктор.

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 проєктору.

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 12.1. Криміналістичні дослідження електронної пошти**

Навчальна мета заняття: отримати навички криміналістичного дослідження електронної пошти.

Кількість годин: 4 год.

Навчальні питання

1. Сценарій кримінальної події Email Harassment.
2. Криміналістичне дослідження електронної пошти.

Література:

1. Керівництво до практичних і лабораторних занять.
2. <https://digitalcorpora.org/corpora/scenarios/nitroba-university-harassment-scenario>

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

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 13.1. 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, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна

1. EC-Council. Computer Hacking Forensic Investigator v9. Courseware.
2. 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.
3. 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.
4. 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.

Додаткова

5. Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Third Edition. Edited by Eoghan Casey. www.elsevierdirect.com/companions/9780123742681.
6. Handbook of Digital Forensics and Investigation Edited by Eoghan Casey. <http://www.elsevierdirect.com/product.jsp?isbn=9780123742674>.
7. 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>.
8. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition (Information Security) Auerbach Publications; 2 edition (December 19, 2007).
9. Good Practice Guide for Computer-Based Electronic Evidence. Official release version 4.0. Published by 7Safe. www.7safe.com
10. Dan Farmer, Wietse Venema. Forensic Discovery. Pearson Education, Inc., December 2004.
11. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.
12. Davidoff, Sherri. Network forensics : tracking hackers through cyberspace / Sherri Davidoff, Jonathan Ham. Pearson Education, Inc. 2012.

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>