**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**
**ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ «РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»**

Відділення інформаційних технологій
Циклова комісія *програмування та інформаційних дисциплін*

**ЗАТВЕРДЖУЮ**
Заступник директора
з навчально-виробничої роботи
_____ 2025 р.
_____ Тарас САСОВСЬКИЙ

# ПРОГРАМА ПРАКТИКИ

| ***Розслідування інцидентів кіберзлочинів*** | |
|---|---|
| галузь знань | *І2 Інформаційні технології* |
| спеціальність | *125 Кібербезпека та захист інформації* |
| освітня програма | *Кібербезпека та захист інформації* |

Рівне – 2025 рік

Програма практики з *РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ КІБЕРЗЛОЧИНІВ* розроблено на основі освітньо-професійної програми *Кібербезпека та захист інформації* для здобувачів освіти освітньо-професійного ступеня "Фаховий молодший бакалавр" галузі знань 12 Інформаційні технології, спеціальності *125 Кібербезпека та захист інформації, затвердженої Вченою радою НУБіП України протокол від 26.04.2023 №10*

Розробники: *Янок Назар Сергійович, спеціаліст, викладач програмування та інформаційних дисциплін;*

Програму навчальної дисципліни розглянуто і схвалено на засіданні циклової комісії *програмування та інформаційних дисциплін*

Протокол від «29» серпня 2025 року № 1

Голова циклової комісії *програмування та інформаційних дисциплін*

«29» серпня 2025 року _____ *Павло СТРИК*

Погоджено методичною радою ВСП «РФК НУБіП України»

Протокол від «29» *серпня* 2025 року № 1

29 серпня 2025 року Голова _____ *Людмила БАЛДИЧ*

# ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| **Галузь знань, напрям підготовки, спеціальність, освітньо-професійний ступінь** | |
|---|---|
| Освітньо-професійний ступінь | *фаховий молодший бакалавр* |
| Галузь знань | *12 Інформаційні технології* |
| Спеціальність | *125 Кібербезпека та захист інформації* |
| **Характеристика навчальної дисципліни** | |
| Вид | обов’язкова |
| Загальна кількість годин | 135 |
| Кількість кредитів ECTS | 4,5 |
| Кількість змістових модулів | 3 |
| Мова викладання, навчання та оцінювання | українська |
| Форма контролю | Залік з практики |
| **Показники навчальної дисципліни для денної форми навчання** | |
| Форма навчання | денна |
| Рік підготовки | 2025-2026 |
| Семестр | 6 |
| Аудиторні години: | 54 |
| Самостійна робота, год | 81 |

# МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**Мета навчальної дисципліни** полягає в поглибленні теоретичної і практичної підготовки фахівця, спрямованої на вирішення типових та складних завдань цифрової криміналістики, що полягають у зборі цифрової криміналістичної інформації, збереженні, дослідженні і використанні цифрових доказів.

**Завдання навчальної дисципліни:**

- ознайомлення з основними поняттями кіберзлочинності та цифрової криміналістики;
- вивчення методів та інструментів цифрових розслідувань, що застосовуються у кіберзлочинах;
- розгляд класифікації кіберзлочинів та основних способів їхнього вчинення;
- освоєння методології збору, аналізу та збереження цифрових доказів;
- вивчення принципів роботи з цифровими доказами та їхньої правової значущості;
- навчання проведенню експертизи даних, відновленню видаленої інформації та аналізу цифрових слідів;
- дослідження способів приховування цифрових слідів та методів антикриміналістики;
- аналіз методів розслідування атак на комп'ютерні системи та мережі;
- ознайомлення з особливостями аналізу мобільних пристроїв у кіберрозслідуваннях;
- опрацювання методів виявлення та протидії стеганографії й шифруванню;
- вивчення методів атрибуції кіберзлочинців та аналізу цифрового місця злочину;
- засвоєння принципів експертної оцінки цифрових доказів та складання звітів;
- розгляд автоматизованих систем аналізу кіберзлочинів та їхніх можливостей.

**вміти:**

- визначати основні види кіберзлочинів та їхні характеристики;
- застосовувати методи збору, аналізу та збереження цифрових доказів;
- працювати з програмними та апаратними засобами цифрової криміналістики;
- аналізувати файлові системи, дискові структури та процеси завантаження операційних систем;
- відновлювати видалені дані та перевіряти їхню цілісність за допомогою хеш-функцій;
- проводити розслідування мережевих атак та аналізувати трафік;
- здійснювати криміналістичний аналіз мобільних пристроїв та хмарних сервісів;

- виявляти приховані та зашифровані дані, застосовувати методи стеганоаналізу;
- використовувати інструменти цифрової криміналістики для аналізу логів, реєстрів та метаданих;
- ідентифікувати способи уникнення цифрового сліду та протидіяти антикриміналістиці;
- проводити експертну оцінку цифрових доказів та складати висновки;
- використовувати моделі розслідування кіберзлочинів та планувати аналітичні розслідування.

**Очікувані результати навчання.**

Після вивчення дисципліни «Розслідування інцидентів кіберзлочинів» у здобувачів освіти формуються такі **компетентності:**

**Загальні (ЗК):**

**ЗК01.** Здатність застосовувати знання у практичних ситуаціях.

**ЗК05.** Знання та розуміння предметної області та розуміння професійної діяльності.

**Спеціальні (ФК):**

**ФК04.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

**ФК06.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

**ФК08.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

**ФК12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

**Програмні результати навчання (ПР):**

**ПР15.** Вміти вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

**ПР16.** Вміти вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків.

**ПР17.** Вміти вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

# ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**Тема 1. Організаційна частина. мета та завдання навчальної практики**

Вступ. Ознайомлення з робочою програмою практики. Інструктаж з техніки безпеки згідно з вимогами охорони праці. Підготовка робочого місця та обладнання.

**Тема 2. Поглиблене вивчення і здобуття навиків з розслідування кіберзлочинів**

Цифрова криміналістика та методи розслідування кіберзлочинів; правові та етичні аспекти збору й зберігання цифрових доказів; методи аналізу мережевих та системних артефактів; статичний і динамічний аналіз шкідливого ПЗ; використання Threat Intelligence для кореляції й виявлення загроз.

**Тема 3. Основи комп'ютерної криміналістики**

Моніторинг та реагування на кіберінциденти; архітектура SIEM та збір логів; аналіз журналів подій і кореляція подій; виявлення та реагування на інциденти (Incident Response); threat hunting і пошук прихованих загроз; звітування та відновлення після інциденту.

**Тема 4. Захист звітів**

Опис результатів виконаних робіт. Демонстрація оформленого друкованого звіту згідно діючих інструкцій та вимог.

# ТЕМАТИЧНИЙ ПЛАН

| № | Назви тем практики | Кількість годин | | |
|---|---|---|---|---|
| | | денна форма | | |
| | | всього | аудиторні | самостійне вивчення |
| *1* | *2* | *3* | *4* | *5* |
| **Змістовий модуль 1. ОРГАНІЗАЦІЙНА ЧАСТИНА** | | | | |
| ***Тема 1*** | Техніка безпеки. Мета та завдання навчальної практики. | 5 | 2 | 3 |
| **Разом за змістовим модулем 1** | | **5** | **2** | **3** |
| **Змістовий модуль 2. Поглиблене вивчення і здобуття навиків з розслідування кіберзлочинів** | | | | |
| *Тема 2* | Розслідування кіберзлочинів методами цифрової криміналістики | 63 | 25 | 38 |
| *Тема 3* | Моніторинг та реагування на кіберінциденти | 63 | 25 | 38 |
| **Разом за змістовим модулем 2** | | **126** | **50** | **76** |
| **Змістовий модуль 3 . ЗАХИСТ ЗВІТІВ** | | | | |
| *Тема 4* | Захист звітів | 4 | 2 | 2 |
| **Разом за змістовим модулем 3** | | **4** | **2** | **2** |
| **Всього годин** | | **135** | **54** | **36** |

## 5. Календарно-тематичний план навчальної практики

| № занят тя | Тижні | | Назва розділу, теми і зміст практики | Кількість годин | | Місце та об'єкт проведення | Інструменти, матеріали, та обладнання | Організація форми робіт | Завдання на самостійне опрацювання | Примітка |
|---|---|---|---|---|---|---|---|---|---|---|
| | № | Дата | | всього | ауди-торних | | | | | |
| **1** | **1** | | **Техніка безпеки. Мета та завдання навчальної практики.** Ознайомлення з правилами ТБ та завданнями практики. Підготовка робочого місця та обладнання | 5 | 2 | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **2** | **1** | | **Цифрова криміналістика та методи розслідування кіберзлочинів.** Опис інциденту та збір початкових даних, Аналіз методів атаки (Tactics & Techniques), Індикатори компрометації (IoC), Трасування інфраструктури загроз, Відновлення ходів зловмисника (Threat Hunting), Побудова профілю загрози (Threat Actor Profiling) | **5** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **3** | **1** | | **Розслідування компрометації через зловмисне браузерне розширення.** Опис інциденту та збір мережевих даних, Попередня обробка та фільтрація PCAP-файлів, Аналіз мережевого трафіку .Ідентифікація індикаторів компрометації (IP, домени, протоколи), Кореляція з Threat Intelligence (репутаційні бази, звіти), Визначення векторів проникнення та рекомендації з усунення й захисту. | **6** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **4** | **1** | | **Встановлення обставин інциденту та збір початкової інформації.** Аналіз PCAP-файлів для виявлення аномального трафіку. Визначення вектору атаки та способу проникнення. Виявлення індикаторів компрометації (IoC). Залучення Threat Intelligence для | **5** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | підтвердження загроз. Формування висновків та рекомендацій щодо реагування. | | | | | | | |
| **5** | **1** | | **Аналіз шкідливого виконуваного файлу за хешем та виявлення зв'язку з C2-інфраструктурою.** Збір базової інформації про підозрілий файл. Визначення хешу та перевірка через Threat Intelligence сервіси. Ідентифікація типу шкідливого ПЗ та його функцій. Виявлення зв'язку з Command and Control (C2) інфраструктурою. Кореляція з відомими кампаніями та попередніми інцидентами. Формування рекомендацій для команди реагування та SOC. | **6** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **6** | **2** | | **Розслідування потенційної supply chain-атаки через скомпрометоване оновлення 3CX Desktop App** | **5** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **7** | **2** | | **Аналіз зразка IcedID та моніторинг діяльності APT-групи, що використовує фішингові кампанії** | **5** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **8** | **2** | | **Розслідування підозрілої активності в мережевому трафіку та оцінка ризику витоку даних в онлайн-магазині** | **6** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **9** | **2** | | **Аналіз дампу пам'яті для виявлення дій шкідливого ПЗ на зараженій робочій станції** | **6** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **10** | **2** | | **Розслідування бокового руху в мережі з використанням PsExec за даними PCAP** | **6** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **11** | **3** | | **Аналіз підозрілого PPT-файлу, отриманого через фішинговий лист, та виявлення ознак шкідливої активності** | **5** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **12** | **3** | | **Цифровий аналіз мобільного пристрою в межах** | **5** | **4** | аудиторія КІЦ ВСП «РФК | мультимедійний проектор, комп'ютери та | індивідуальна | оформити звіт-щоденник практики | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **розслідування злочину** | | | НУБіП України» | програмне забезпечення | | | |
| **13** | **3** | | **Розслідування інциденту з перенаправленням трафіку на сторонні ресурси в мережі GlobalTech Industries** | **5** | **2** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **14** | **3** | | **Аналіз компрометації веб-сервера Apache Tomcat на основі мережевого трафіку (PCAP)** | **5** | **2** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **15** | **3** | | **Захист звітів.** Оформлення щоденнику-звіту з дотриманням рекомендацій. Захист звітів | **6** | **4** | аудиторія КІЦ ВСП «РФК НУБіП України» | мультимедійний проектор, комп'ютери та програмне забезпечення | індивідуальна | оформити звіт-щоденник практики | |
| **Всього** | | | | **81** | **54** | | | | | |

# 6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

| *№* | *Тема дисципліни* | *Вид завдання (реферати, дослідницькі, розрахункові роботи тощо)* | *Календарні строки і форма контролю* |
|---|---|---|---|
| 1 | Типологія кіберзлочинів: класифікація та приклади | реферат | 3 тижні |
| 2 | Роль цифрової криміналістики у сучасних кіберрозслідуваннях | реферат | 3 тижні |
| 3 | Міфи про кіберзлочинність у мас-медіа та їх спростування | реферат | 3 тижні |
| 4 | Методи збору та документування цифрових доказів | реферат | 3 тижні |
| 5 | Особливості збереження та вилучення цифрових доказів з різних пристроїв | реферат | 3 тижні |
| 6 | Логічна та фізична структура жорстких дисків у цифровій криміналістиці | реферат | 3 тижні |
| 7 | Методи виявлення та аналізу прихованих розділів (DCO, HPA) | реферат | 3 тижні |
| 8 | Аналіз процесу завантаження ОС та виявлення маніпуляцій | реферат | 3 тижні |
| 9 | Види цифрових доказів та їх джерела (локальні, хмарні, IoT) | реферат | 3 тижні |
| 10 | Аналіз логів, історії браузера та EXIF-метаданих у розслідуваннях | реферат | 3 тижні |
| 11 | Геолокація та її роль у встановленні місцезнаходження підозрюваних | реферат | 3 тижні |
| 12 | Методологія розслідування кіберзлочинів на місці події | реферат | 3 тижні |
| 13 | Засоби фіксації, збереження та захисту цифрових доказів | реферат | 3 тижні |
| 14 | Огляд інструментів для цифрової криміналістики (FTK Imager, Autopsy тощо) | реферат | 3 тижні |
| 15 | Хеш-функції у цифровій криміналістиці: принципи та застосування | реферат | 3 тижні |
| 16 | Аналіз реєстру Windows і журналів подій як джерело цифрових доказів | реферат | 3 тижні |
| 17 | Методи виявлення мережевих атак: DDoS, MITM, SQLi | реферат | 3 тижні |
| 18 | Використання Wireshark, Zeek, Suricata для збору мережевих доказів | реферат | 3 тижні |
| 19 | Методи вилучення та аналізу даних з мобільних пристроїв | реферат | 3 тижні |
| 20 | Шифрування, стеганографія та приховані потоки даних у кіберзлочинності | реферат | 3 тижні |
| 21 | Аналіз rootkits, bootkits та способи їх виявлення | реферат | 3 тижні |
| 22 | Методи уникнення цифрового сліду: VPN, TOR, анонімні мережі | реферат | 3 тижні |
| 23 | Огляд моделей розслідування кіберзлочинів (IDIP, EIDIP, HOBFDIP) | реферат | 3 тижні |
| 24 | Методи атрибуції кіберзлочинців: проблеми, техніки, приклади | реферат | 3 тижні |
| 25 | Застосування OSINT у кіберрозслідуваннях | реферат | 3 тижні |

| | | | |
|---|---|---|---|
| 26 | Автоматизовані системи та штучний інтелект у розслідуванні кіберзлочинів | реферат | 3 тижні |
| 27 | Роль Big Data у прогнозуванні та профілактиці кіберзлочинів | реферат | 3 тижні |
| 28 | Аналіз кіберзлочинів у державному, корпоративному та приватному секторах | реферат | 3 тижні |
| 29 | Методи відновлення видалених даних у цифровій криміналістиці | реферат | 3 тижні |
| 30 | Побудова цифрового профілю зловмисника на основі відкритих даних | реферат | 3 тижні |

# 7. Контроль результатів навчання

## 7.1. Форми та засоби поточного і підсумкового контролю

Контроль знань здобувачів освіти здійснюється за модульно-рейтинговою системою.

Засобами діагностики та методами демонстрування результатів навчання здобувачів освіти з дисципліни є:

- індивідуальне опитування;
- презентація змісту практики;
- захист звіту практики;
- залік з практики.

## 7.2 Критерії оцінювання результатів начиння

**Оцінка «відмінно»** виставляється студенту, який має стійкі системні, глибокі і різнобічні знання, відмінно володіє матеріалом, знає нормативну і законодавчу базу та її застосування за певних умов, дає обґрунтовані, правильні відповіді на питання, доцільно використовує термінологію дисципліни (предмета), усвідомлює взаємозв'язок окремих розділів дисципліни, їхнє значення для майбутньої професії, виявляє творчі здібності у розумінні та використанні навчально-програмного матеріалу, проявляє здатність до самостійного оновлення і поповнення знань. Практичні завдання і задачі вирішує правильно, розрахунки проводить без помилок, отримує достовірні результати, правильно заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- глибоке, теоретично обґрунтоване розкриття питання; розрахунки, зроблені без помилок, проведено повний аналіз, відображена власна позиція – оцінюються в **48-50 балів;**

- обґрунтоване розкриття питання чи/та розрахунки, зроблені з незначними неточностями, які істотно не впливають на правильність відповіді – **45-47 балів;**

**Оцінка «добре»** виставляється студенту, який знає викладений матеріал і добре ним володіє але допускає незначні помилки у формулюванні термінів, категорій, понять, використанні нормативно-правової бази, показує стійкий рівень знань з дисципліни і та професійної діяльності. Під час виконання практичних завдань, вирішення задач, проведення розрахунків допускає незначні помилки, але за допомогою викладача швидко орієнтується і знаходить правильні відповіді, правильно або з незначними помилками заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- відповідь не дає повного розкриття питання, не проведено повний аналіз результатів розрахунків, немає власної позиції – **42-44 балів;**

- неповне розкриття питання, доведені до завершення розрахунки але не зроблено їх аналіз; загалом наявні достатні знання – **38-41 балів;**

**Оцінка «задовільно»** виставляється студенту, який посередньо володіє матеріалом, виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та наступної роботи за професією, справляється з виконанням завдань, передбачених програмою, дає неправильну відповідь на окремі питання або на всі питання дає малообґрунтовані, невичерпні відповіді, знання має обмежені, несистемні, слабо орієнтується у нормативно-правових документах. Під час виконання практичних завдань, вирішення задач, проведення розрахунків припускається грубих помилок і тільки за допомогою викладача може виправити допущені помилки, із значними помилками заповнює і складає документи, поверхово робить узагальнення і висновки та не зовсім охайно оформляє виконані завдання та звіти. - питання розкрите фрагментарно, наявні фактологічні помилки під час викладу чи/та помилки під час проведення розрахунків – **34-37 балів;**

- відповідь неповна, наявні суттєві помилки при викладі та проведенні розрахунків – **30-33 балів;**

**Оцінка «незадовільно»** виставляється студенту, який не виявив достатніх знань основного навчально-програмного матеріалу, дає відповіді лише на деякі питання або дає неправильні відповіді на питання, може відтворити кілька термінів, не знає термінології дисципліни і основних нормативно-правових документів, не може без допомоги викладача використати знання у подальшому навчанні, не спромігся оволодіти навичками самостійної роботи. Допускає принципові помилки у виконанні передбачених програмою завдань, вирішенні задач, проведенні розрахунків припускається грубих помилок і не може їх виправити, не виконує практичне завдання у визначений термін, із значними помилками заповнює і складає документи, не робить узагальнення і висновки та не охайно оформляє виконані завдання та звіти.

- відповідь має значні помилки елементарного рівня – **1-30 бали;**
- відсутність відповіді на питання – **0 балів.**

## 7.3. Оцінювання за формами контролю

| | Заліковий модуль 1 | Заліковий модуль 2 | Заліковий модуль (залік) | Разом |
|---|---|---|---|---|
| % | 20 | 20 | 40 | 100 |
| Мінімум | 0 | 0 | 0 | 0 |
| Максимум | 50 | 50 | 50 | 50 |

## 7.4 Шкала оцінювання

| **Відсоток формування компетентностей та набуття програмних результатів навчання** | **Рейтинг за п’ятдесятибальною шкалою** | **Оцінка за п’ятибальною шкалою** | **Запис у заліковій книжці студента та відомості** |
|---|---|---|---|
| 96-100 | 48, 49, 50 | 5 | відмінно |

| | | | |
|---|---|---|---|
| 90-95 | 45, 46, 47 | 5 | відмінно |
| 84-89 | 42, 43, 44 | 4 | добре |
| 75-83 | 38, 39, 40, 41 | 4 | добре |
| 67-74 | 34, 35, 36, 37 | 3 | задовільно |
| 60-66 | 30, 31, 32, 33 | 3 | задовільно |
| менше 60 | 0-29 | 2 | незадовільно |

## 11. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

### Основна література:


1. Гончаров С. В. Цифрова криміналістика: навч. посіб. / С. В. Гончаров. – Харків: ХНУВС, 2020. – 248 с.
2. Романюк Л. М., Коваленко А. С. Основи комп'ютерної криміналістики / Л. М. Романюк, А. С. Коваленко. – Київ: НАВС, 2021. – 312 с.
3. Nelson B., Phillips A., Steuart C. Guide to Computer Forensics and Investigations. – Boston: Cengage Learning, 2019. – 832 p.
4. Nikkel B. Digital Forensics: Threatscape and Best Practices. – Hoboken: Wiley, 2020. – 352 p.


### 5. Допоміжні


6. Sammons J. The Basics of Digital Forensics. – 3rd ed. – [s.l.]: Syngress, 2020. – 240 p.
7. Altheide C., Carvey H. Digital Forensics with Open Source Tools. – 2nd ed. – [s.l.]: Syngress, 2020. – 288 p.
8. Holt T. J., Bossler A. M. Cybercrime and Digital Forensics. – 3rd ed. – New York: Routledge, 2022. – 400 p.
9. Quick D., Choo K.-K. R. Digital Forensics and Investigation. – Cham: Springer, 2020. – 275 p.
10. Applied Cyber Forensics / ed. E. E. Kenneally. – Cham: Springer, 2021. – 298 p.
11. Handbook of Digital Forensics and Investigation / ed. H. Bidgoli. – Boston: Cengage, 2020. – 540 p.