МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«30» 08 2024 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«30» 08 2024 р.

ЗАТВЕРДЖУЮ
Директор навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
«30» 08 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Цифрова криміналістика»
ступінь вищої освіти – магістр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. роботи (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік / екзамен (семестр)
ДФН	1	2	30	14	4	6	96	150	Залік (2)
ЗФН	1	3	8	4	-	-	138	150	Залік (3)

30.08.2024

Тернопіль – 2024

Робоча програма розроблена на основі освітньо-професійної програми підготовки магістра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації», затвердженої Вченою радою ЗУНУ (протокол № 11 від 23.06.2024 р.).

Робочу програму склав старший викладач кафедри кібербезпеки, доктор філософії (спеціальність 125 - Кібербезпека та захист інформації) Сергій КУЛИНА.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «Кібербезпека та захист інформації», протокол №1 від 30.08.2024 р.

Голова групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант освітньо-професійної
програми Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “Цифрова криміналістика”

Дисципліна – Цифрова криміналістика	Галузь знань, спеціальність, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів – 5	Галузь знань 12 Інформаційні технології	Статус дисципліни – обов’язкова Мова навчання - українська
Кількість залікових модулів –3	Спеціальність 125 – Кібербезпека та захист інформації	Рік підготовки: ДФН – 1; ЗФН – 1. Семестр: ДФН – 2; ЗФН – 3.
Кількість змістових модулів –3	Ступінь вищої освіти – магістр	Лекції: ДФН –30 год.; ЗФН – 8 год. Лабораторні заняття: ДФН – 14 год.; ЗФН – 4 год.
Загальна кількість годин – 150		Індивідуальна робота: ДФН - 4 год. Тренінг: ДФН - 6 год. Самостійна робота: ДФН – 96 год.; ЗФН – 138 год.
Тижневих годин:15 год., з них аудиторних –3 год.		Вид підсумкового контролю – залік

2. Мета й завдання вивчення дисципліни “Цифрова криміналістика”

2.1. Мета завдання дисципліни

Мета вивчення дисципліни “Цифрова криміналістика” полягає у формуванні у майбутніх спеціалістів умінь та компетентностей для забезпечення ефективного захисту інформації з використанням сучасних систем цифрової криміналістики, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів сучасних методів та методик аналізу ризиків, оцінювання управління ризиками в умовах широкого використання інформаційних технологій.

2.2 **Завдання вивчення дисципліни**

Основне завдання курсу є вироблення у студентів вміння застосовувати нові методи в дослідницькій і прикладній діяльності сучасний системи цифрової криміналістики; здійснювати аналіз ризиків функціонування комп’ютерних систем: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання управління ризиками; здійснювати систематичний збір і обробку інформації, яка може бути використана для підвищення захищеності мережі, процесу ухвалення

рішення, оцінки програм або вироблення політики безпеки; застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки.

2.3.Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

- Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
- Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

2.4 Передумови для вивчення дисципліни.

Вивчення курсу "Цифрова криміналістика" передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Тестування комп'ютерних систем на проникнення», «Моніторинг та управління інформаційною безпекою»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.5. Програмні результати навчання:

- Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
- Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
- Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
- Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

3. Програма навчальної дисципліни "Цифрова криміналістика"

Змістовий модуль 1. Загальні положення цифрової криміналістики

Тема 1. Концептуальні засади забезпечення інформаційної безпеки України

Нормативно-правові основи захисту інформації в Україні. Концепція національної безпеки України, концепція інформаційної безпеки України, доктрина інформаційної безпеки України. Основні поняття, терміни та визначення. Організація захисту інформації у ОВС України.

Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації

Місце технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації. Основні поняття, терміни та визначення технічного захисту інформації. Види інформації, яка може стати об’єктом злочинних посягань. Поняття технічних каналів витоку інформації та механізм їх утворення. Види та класифікація технічних каналів витоку інформації та способів несанкціонованого зняття інформації. Визначення можливих джерел витоку акустичної та електромагнітної інформації у приміщенні.

Тема 3. Методи та засоби блокування технічних каналів витоку інформації

Порядок проведення та складові ТЗІ у підрозділах ОВС України. Методи пасивного та активного захисту інформації. Методи та засоби захисту акустичної інформації. Методи та засіб захисту електромагнітної інформації. Методи захисту від ВЧ-нав’язування.

Тема 4. Поняття та кримінологічна характеристика кіберзлочинності

Визначення та ознаки кіберзлочинності. Класифікація кіберзлочинів. Кримінологічна характеристика кіберзлочинності.

Тема 5. Розслідування кіберзлочинів

Процедура розслідування комп'ютерних інцидентів. Проведення аналізу причин та умов ІТ-інцидентів. Виявлення обставини комп'ютерних злочинів за допомогою сучасних засобів. Вразливість інформаційних систем, наявність каналів витоку інформації, вплив людського чинника, апаратні збої інформаційних систем та інші порушення інформаційної безпеки.

Змістовий модуль 2. Технічні засоби цифрової криміналістики

Тема 6. Засоби стирання, видалення даних та інформації

Пристрої для знищення цифрової інформації з використанням програмних засобів, а також апаратні засоби для миттєве знищення даних на магнітних носіях без можливості відновлення.

Тема 7. Засоби копіювання даних

Засоби копіювання даних на HDD. Копіювання даних на телефонах. Тиражування дисків. Виготовлення необмеженої кількості копій жорстких дисків за короткий час.

Тема 8. Обладнання для блокування запису

Принципи функціонування апаратних блокаторів запису. Принципи функціонування апаратних блокаторів записи. Принципи тестування апаратних блокаторів запису. Методика тестування апаратних блокаторів запису.

Тема 9. Аналіз зібраної інформації

Аналізатори протоколів. Пристрої для аналізу протоколів інтерфейсу ATA, призначені для реєстрації та відображення команд і даних, що передаються між будь-якими пристроями з

інтерфейсами Parallel ATA або Serial ATA.

Тема 10. Відновлення даних

Системи відновлення даних комп'ютерної криміналістики. спеціалізовані пристрої відновлення даних з комп'ютерної техніки, систем зберігання даних, відеореєстраторів, мобільних телефонів та інших портативних пристроїв.

Змістовний модуль 3. Програмне забезпечення цифрової криміналістики

Тема 11. Продукти аналізу і обробки ризиків інформаційної безпеки

Функціональні можливості для виявлення і зменшення ризиків. Перевірка відповідності різноманітним стандартам інформаційної безпеки (Rapid7).

Тема 12. Оцінка захищеності інформаційних систем від несанкціонованого доступу та інших загроз інформаційній безпеці

Пошук вразливості периметра комп'ютерної мережі, визначення можливих каналів витоку інформації та оцінка ризиків інформаційної безпеки. Пошук та керування вразливостями.

Тема 13. ПЗ для розслідування комп'ютерних злочинів

Програмно-апаратні засоби моніторингу використання ресурсів Інтернет, запобігання витоку інформації, аналіз та відновлення втрачених даних. Decision Group. Guidance Software Inc.

Тема 14. Апаратно-програмні засоби шифрування мобільного зв'язку

Засоби шифрування мобільного зв'язку: дзвінків, повідомлень SMS та електронної пошти.

Тема 15. Захищені модульні системи зберігання даних

Захищені модульні системи зберігання даних, засоби шифрування інформації на накопичувачах, дублікатори та перетворювачі інтерфейсів. Addonics.

4. Структура залікового кредиту дисципліни "Цифрова криміналістика"

ДФН

<table>
<tr><td rowspan="2">Тема</td><td colspan="6">Кількість годин</td></tr>
<tr><td>Лекції</td><td>Практ. заняття</td><td>ІРС</td><td>Тренінг</td><td>СРС</td><td>Контр. заходи</td></tr>
<tr><td colspan="7">Змістовий модуль 1. Загальні положення цифрової криміналістики</td></tr>
<tr><td>Тема 1. Концептуальні засади забезпечення інформаційної безпеки України.</td><td>2</td><td rowspan="6">2</td><td rowspan="6">1</td><td rowspan="6">2</td><td>6</td><td rowspan="6">Поточне опитування</td></tr>
<tr><td>Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації.</td><td>2</td><td>6</td></tr>
<tr><td>Тема 3. Методи та засоби блокування технічних каналів витоку інформації.</td><td>2</td><td>6</td></tr>
<tr><td>Тема 4. Поняття та кримінологічна характеристика кіберзлочинності.</td><td>2</td><td>6</td></tr>
<tr><td>Тема 5. Розслідування кіберзлочинів.</td><td>2</td><td>8</td></tr>
<tr><td colspan="7">Змістовий модуль 2. Технічні засоби цифрової криміналістики</td></tr>
<tr><td>Тема 6. Засоби стирання, видалення даних та інформації.</td><td>2</td><td>2</td><td>1</td><td>2</td><td>6</td><td>Поточне опитування</td></tr>
</table>

Тема 7. Засоби копіювання даних	2				6	
Тема 8. Обладнання для блокування запису	2				6	
Тема 9. Аналіз зібраної інформації.	2	4			6	
Тема 10. Відновлення даних	2				8	
Змістовий модуль 3. Програмне забезпечення цифрової криміналістики						
Тема 11. Продукти аналізу і обробки ризиків інформаційної безпеки.	2				6	
Тема 12. Оцінка захищеності інформаційних систем від несанкціонованого доступу та інших загроз інформаційній безпеці.	2	2	1		6	
Тема 13. ПЗ для розслідування комп'ютерних злочинів	2			2	6	Поточне опитування
Тема 14. Апаратно-програмні засоби шифрування мобільного зв'язку.	2				6	
Тема 15. Захищені модульні системи зберігання даних	2	2	1		8	
Разом	30	14	4	6	96	

ЗФН

Тема	Кількість годин		
	Лекції	Практичні заняття	СРС
Змістовий модуль 1. Загальні положення цифрової криміналістики			
Тема 1. Концептуальні засади забезпечення інформаційної безпеки України.			10
Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації.			8
Тема 3. Методи та засоби блокування технічних каналів витоку інформації.	2	-	8
Тема 4. Поняття та кримінологічна характеристика кіберзлочинності.			8
Тема 5. Розслідування кіберзлочинів.			12
Змістовий модуль 2. Технічні засоби цифрової криміналістики			
Тема 6. Засоби стирання, видалення даних та інформації.			10
Тема 7. Засоби копіювання даних.			8
Тема 8. Обладнання для блокування запису.	2	2	8
Тема 9. Аналіз зібраної інформації.			8
Тема 10. Відновлення даних.			12
Змістовий модуль 3. Програмне забезпечення цифрової криміналістики			
Тема 11. Продукти аналізу і обробки ризиків інформаційної безпеки.			10
Тема 12. Оцінка захищеності інформаційних систем від несанкціонованого доступу та інших загроз інформаційній безпеці.	4	2	8
Тема 13. ПЗ для розслідування комп'ютерних злочинів.			8
Тема 14. Апаратно-програмні засоби шифрування мобільного			8

зв'язку.			
Тема 15. Захищені модульні системи зберігання даних.			12
Разом	8	4	138

5. Тематика практичних занять

Лабораторна робота № 1

Тема: Практичний пошук можливих джерел витоку інформації.

Мета: Навчитися виконувати пошук можливих джерел витоку інформації по технічних каналах витоку.

Питання для обговорення: Витік інформації. Можливі канали витоку і несанкціонованого доступу до інформації. Канали витоку інформації.

Лабораторна робота № 2

Тема: Практичне застосування методик і засобів пошуку радіозакладних пристроїв.

Мета: Використання засобів пошуку радіозакладних пристроїв.

Питання для обговорення: Комплекс проблем, пов'язаних з пошуком та локалізацією радіозакладних пристроїв. виявлення радіозакладних пристроїв, що використовують різного роду складні або шумоподібні сигнали, а також надкороткі передачі. Описані методи локалізації та виявлення радіозакладок і апаратура, яка для цього призначена, з врахуванням пошуку радіовипромінювань, аналізу та їх обробки з метою встановлення належності

Лабораторна робота № 3

Тема: Розмежування доступу, застосування різних програм шифрування при збереженні інформації на дисках

Мета: Отримання практичних навичок розмежування доступу, застосування антивірусних програм та різних програм шифрування при збереженні інформації на дисках

Питання для обговорення: розмежування доступу, застосування антивірусних програм, застосування програм шифрування при збереженні інформації.

Лабораторна робота № 4

Тема: Стеганографічний захист інформації.

Мета: Практичне ознайомлення з методами та програмами стеганографічного захисту інформації, в тому числі у мережі.

Питання для обговорення: математичні основи стеганографічного захисту інформації, методи вбудовування інформації в файли та їх використання, оцінка стійкості методів вбудовування інформації.

Лабораторна робота № 5

Тема:. Використання методів шифрування даних.

Мета: Ознайомлення та отримання практичних навичок використання методів та практичних програмам шифрування

Питання для обговорення: Методи шифрування. Стандарти шифрування. Шифрування з відкритим ключем.

Лабораторна робота № 6

Тема: Технології реалізації систем захисту інформації.

Мета: Практичне ознайомлення з Технологіями реалізації систем захисту інформації у мережах на прикладі сучасного програмного забезпечення.

Питання для обговорення: Технології захисту інформації. Системи захисту інформації.

6. Самостійна робота

Самостійне завдання студента полягає у виконанні обраного та підтвердженого викладачем наскрізного завдання.

Метою виконання самостійної роботи є дослідження ступеня захищеності інформаційного об’єкта та пошук цифрових доказів зміни його стану. Студенти повинні обрати одну із запропонованих тематик:

Тематика

1	Проблеми захисту інформації у сучасних ІС.
2	Види комп’ютерних злочинів та причини поширення комп’ютерної злочинності
3	Поняття і класифікація комп’ютерних вірусів.
4	Засоби захисту інформації.
5	Архівування та резервне копіювання даних.
6	Захист вмісту зовнішньої пам'яті.
7	Захист програмного забезпечення.
8	Захист даних від шкідливих програм.
9	Поширені види мережевих атак і способи захисту від них.
10	Організація бездротового зв'язку, специфічні атаки на бездротові мережі та способи захисту від них.

7. Організація та проведення тренінгу з дисципліни «Цифрова криміналістика»

Тематика: Задача аналізу та класифікації погроз. Групування суб’єктів та об’єктів доступу.

Порядок проведення:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.
2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.
3. Практична частина реалізується шляхом виконання завдань за темами тренінгу.
4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Перелік питань для тренінгу:

1. Дослідження даних, розміщених на змінних носіях та жорсткому диску.
2. Дослідження даних операційної системи Windows.
3. Дослідження даних операційної системи Linux.

8. Методи навчання

У навчальному процесі використовуються: лекції, практичні та індивідуальні заняття, групова робота, реферування, а також методи опитування, тестування тощо.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни “Цифрова криміналістика” використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне тестування та поточне опитування;
- підсумкове модульне тестування та опитування за кожним заліковим модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання відповідей на питання тренінгу;
- оцінювання самостійної роботи.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Цифрова криміналістика» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

Модуль 1		Модуль 2	Модуль 3
40%	40%	5%	15%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 1-6.	Підсумкове модульне тестування за темами №1-15.	Оцінка за тренінг визначається як середнє арифметичне за виконання завдань тренінгу за темами 1-3.	Визначається як оцінка за наскрізне завдання самостійної роботи.

Шкала оцінювання

За шкалою ЗУНУ (сума балів за всі види навчальної діяльності в межах модуля)	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	**A** (відмінно)
85–89	добре	**B** (дуже добре)
75–84		**C** (добре)
65–74	задовільно	**D** (задовільно)
60–64		**E** (достатньо)
35–59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1–34		**F** (незадовільно з обов’язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна.

№	Найменування	Номер теми
1.	Електронний варіант лекцій	1-15
2.	Інструкції до виконання практичних робіт (електронний варіант)	1-6
3	Обладнання: Проектор, комп'ютери з доступом до мережі Інтернету. Пограмне забезпечення: FoxitReader, WinZip, Total Commander, Dev C++, Python 3.5.8, Visual Studio community edition.	1-6

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Думчиков М. О. Процеси діджиталізації і криміналістика: ректроспективний аналіз. Криміналістика і судова експертиза. 2020. Вип. 65. С. 100-108.
2. Шепітько В. Ю., Шепітько М. В. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. Право України. 2021. № 8. С. 12-27.
3. Adedoyin, F. F., & Christiansen, B. (2023). Effective cybersecurity operations for Enterprise-Wide systems. Information Science Reference. 2023. - 344 p.
4. Alexandrou, A. (2021). Cybercrime and internet technology: Theory and Practice. CRC Press, 2022. - 455 p.
5. AlFardan, N. (2023). Cyber threat hunting. Manning, 2023. - 442 p.
6. Alsmadi, I., Easttom, C., & Tawalbeh, L. (2020). The NICE Cyber Security Framework: Cyber Security Management. Springer, 2020. - 271 p.
7. Årnes, A. (2023). Cyber investigations. John Wiley & Sons. 2023. - 272 p.
8. Arvatz, A. (2023). The battle for your computer: Israel and the Growth of the Global Cyber-Security Industry. John Wiley & Sons. 2023. - 318 p.
9. Dr. Hidaia Mahmood Alassouli. (2021). Common Windows, Linux and Web Server Systems Hacking Techniques, 2021. – 171 p.
10. Khaleel Ahmad, M.N. Doja, Nur Izura Udzir, Manu Pratap Singh. - CRC Press, 2019. - 331 p.
11. Qc, D. A., Steward, T., & Thakerar, S. (2020). Cyber Risks and Insurance: The Legal Principles. Bloomsbury Professional, 2021. - 227 p.