



Силабус курсу ЦИФРОВА КРИМІНАЛІСТИКА

Ступінь вищої освіти – магістр

Рік навчання: 1,

Семестр: 2

Кількість кредитів: 4

Мова викладання: українська

Керівник курсу

ППП

Сергій Кулина

Контактна інформація

sersks@wunu.edu.ua

Опис дисципліни

Курс «Цифрова криміналістика» знайомить студентів з методами в дослідницькій і прикладній діяльності сучасної системи цифрової криміналістики; аналізом ризиків функціонування комп'ютерних систем: визначення послідовності аналізу, формування моделі порушника та загроз, використання сучасних методів та методик аналізу ризиків, оцінювання управління ризиками; здійснення систематичного збору і обробки інформації, яка може бути використана для підвищення захищеності мережі, процесом ухвалення рішення, оцінки програм або вироблення політики безпеки; застосування національних та міжнародних регулюючих актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/1	Тема 1. Концептуальні засади забезпечення інформаційної безпеки України	Знання концептуальних засад забезпечення інформаційної безпеки України.	Поточне опитування
2/1	Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації	Виявляти шкідливе програмне забезпечення, проводити аналіз шкідливих програм.	Поточне опитування
2/1	Тема 3. Методи та засоби блокування технічних каналів витоку інформації	Розуміти технічні аспекти функціонування шкідливих програм, зменшувати негативні наслідки від впливу шкідливого програмного забезпечення.	Поточне опитування
2/1	Тема 4. Поняття та кримінологічна характеристика кіберзлочинності	Здійснювати аналіз ризиків функціонування комп'ютерних систем.	Поточне опитування
2/1	Тема 5. Розслідування кіберзлочинів	Проводити тестування на проникнення, розробляти методики та процедури реагування на інциденти.	Поточне опитування
2/1	Тема 6. Засоби стирання	Здійснювати систематичний збір і	Поточне

	видалення даних та інформації	обробку інформації, яка може бути використана для оцінки програм або вироблення політики безпеки	опитування
2/1	Тема 7. Засоби копіювання даних	Здійснювати обробку інформації, яка може бути використана при копіюванні даних	Поточне опитування
2/1	Тема 8. Обладнання для блокування запису	Здійснювати систематичний збір і обробку інформації, яка може бути використана для підвищення захищеності мережі та процесу ухвалення рішення.	Поточне опитування
2/1	Тема 9. Аналіз зібраної інформації	Використовувати сучасні методики та стандарти проведення технічного аудиту.	Поточне опитування
2/1	Тема 10. Відновлення даних	Вміння проводити аналіз шкідливих програм.	Поточне опитування
2/1	Тема 11. Продукти аналізу і обробки ризиків інформаційної безпеки	Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/1	Тема 12. Оцінка захищеності інформаційних систем від несанкціонованого доступу та інших загроз інформаційній безпеці	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.	Поточне опитування
2/1	Тема 13. ПЗ для розслідування комп'ютерних злочинів	Збирати та аналізувати докази комп'ютерних злочинів, таких як шахрайство, кібер-шпигунство та інші.	Поточне опитування
2/1	Тема 14. Апаратно-програмні засоби шифрування мобільного зв'язку	Розуміти криміналістичні інструменти та методи, що використовуються для шифрування даних, при передачі лініями мобільного зв'язку.	Поточне опитування
2/1	Тема 15. Захищені модульні системи зберігання даних	Розуміти криміналістичні інструменти та методи, що використовуються для дослідження та аналізу мережевих інцидентів та збереження цифрових доказів	Поточне опитування

Літературні джерела

1. Qc, D. A., Steward, T., & Thakerar, S. (2020). *Cyber Risks and Insurance: The Legal Principles*. Bloomsbury Professional, 2021. — 227 p.
2. Alsmadi, I., Easttom, C., & Tawalbeh, L. (2020). *The NICE Cyber Security Framework: Cyber Security Management*. Springer, 2020. — 271 p.
3. AlFardan, N. (2023). *Cyber threat hunting*. Manning, 2023. — 442 p.
4. Alexandrou, A. (2021). *Cybercrime and internet technology: Theory and Practice*. CRC Press, 2022. — 455 p.
5. Dr. Hidaia Mahmood Alassouli. (2021). *Common Windows, Linux and Web Server Systems Hacking Techniques*, 2021. – 171 p.
6. Adedoyin, F. F., & Christiansen, B. (2023). *Effective cybersecurity operations for*

- Enterprise-Wide systems*. Information Science Reference. 2023. — 344 p.
7. Khaleel Ahmad, M.N. Doja, Nur Izura Udzir, Manu Pratap Singh. — CRC Press, 2019. — 331 p.
 8. Årnes, A. (2023). *Cyber investigations*. John Wiley & Sons. 2023. — 272 p.
 9. Arvatz, A. (2023). *The battle for your computer: Israel and the Growth of the Global Cyber-Security Industry*. John Wiley & Sons. 2023. - 318 p.
 10. Singh, A. P. (2019). *Hacking: the Unlocking of Transparency: Security Is a Myth*. 2019. — 149 p.

Політика оцінювання

Політика щодо запізнення та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Усі письмові роботи перевіряються на наявність плагиату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені.

Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбутись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КППЗ)	Заліковий модуль 4 (письмовий екзамен)
20 %	20 %	20 %	40 %
1. Усне опитування на заняттях: 5 тем по 5 балів – мах 25 балів. 2. Письмова робота – мах 54 балів. 3. Практичне завдання: 3 завдання по 7 бали – мах 21 балів	1. Усне опитування на заняттях: 5 тем по 5 балів – мах 25 балів. 2. Письмова робота – мах 54 балів. 3. Практичне завдання: 3 завдання по 7 бали – мах 21 балів	1. Підготовка КППЗ – мах 40 балів. 2. Захист КППЗ – мах 40 балів. 3. Виконання завдань на тренінгах – мах 20 балів	1. Теоретичні питання: 3 питання по 20 балів - мах 60 балів. 2. Практичне завдання - мах 40 балів

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)