Силабус курсу

ЦИФРОВА КРИМІНАЛІСТИКА

Ступінь вищої освіти – магістр
Рік навчання: 1
Семестр: 2
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП 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/-	Концептуальні засади забезпечення інформаційної безпеки України.	Знання концептуальних засад забезпечення інформаційної безпеки України.	Поточне опитування
2/2	Технічні канали витоку інформації. Способи несанкціонованого зняття інформації.	Виявляти шкідливе програмне забезпечення, проводити аналіз шкідливих програм.	Поточне опитування
2/-	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/-	Поняття та кримінологічна характеристика кіберзлочинності.	Здійснювати аналіз ризиків функціонування комп'ютерних систем.	Поточне опитування
2/2	Розслідування кіберзлочинів.	Проводити тестування на проникнення, розробляти методики та процедури реагування на інциденти.	Поточне опитування

2/-	Засоби стирання, видалення даних та інформації.	Здійснювати систематичний збір і обробку інформації, яка може бути використана для оцінки програм або вироблення політики безпеки	Поточне опитування
2/2	Засоби копіювання даних.	Здійснювати обробку інформації, яка може бути використана при копіюванні даних	Поточне опитування
2/-	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/-	Аналіз зібраної інформації.	Використовувати сучасні методики та стандарти проведення технічного аудиту.	Поточне опитування
2/4	Відновлення даних.	Вміння проводити аналіз шкідливих програм.	Поточне опитування
2/-	Продукти аналізу і обробки ризиків інформаційної безпеки.	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/-	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
2/2	ПЗ для розслідування комп'ютерних злочинів	Збирати та аналізувати докази комп'ютерних злочинів, таких як шахрайство, кібер-шпигунство та інші.	Поточне опитування
2/-	Апаратно-програмні засоби шифрування мобільного зв'язку.	Розуміти криміналістичні інструменти та методи, що використовуються для шифрування даних, при передачі лінями мобільного зв'язку.	Поточне опитування
2/2	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. 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.

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 плагіату 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 відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Модуль 1		Модуль 2	Модуль 4
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)