Силабус курсу

МОНІТОРИНГ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Ступінь вищої освіти – магістр
Рік навчання: 1
Семестр: 1
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП Михайло КАСЯНЧУК
Контактна інформація kmm@wunu.edu.ua

Опис дисципліни

Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області інформаційної безпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних інформаційно-комунікаційних системах та мережах.

Метою викладання дисципліни є розкриття сучасних методів захисту інформації в комп'ютерних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

Структура курсу

Години лек/лаб	Тема	Результати навчання	Завдання
2/-	Постановка задачі аналізу захищеності.	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/2	Збір даних для моніторингу безпеки.	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	Поточне опитування
2/-	Визначення топології та ідентифікація мережевих об'єктів.	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	Поточне опитування
2/2	Ідентифікація сервісів, додатків та ОС.	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики	Поточне опитування

		інформаційної безпеки та/або кібербезпеки організації.	
2/-	Методи ідентифікації вразливостей. passive fingerprinting.	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	Поточне опитування
4/2	Сканери вразливостей. Nessus, Openvas.	Застосовувати сучасні інструменти виявлення вразливостей та їхній подальший аналіз з метою усунення.	Поточне опитування
2/2	Мова опису атак NASL.	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	Поточне опитування
2/-	Інші інструменти аналізу (Xspider, Burp Suite, Nikto, Sqlmap).	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.	Поточне опитування
2/2	Локальний аналіз та захист СУБД.	Застосовувати засоби аналізу та захисту СУБД, усувати ризики та наявні вразливості.	Поточне опитування
2/2	Методології оцінки безпеки (ethical hacking, red/blue/purple teaming).	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	Поточне опитування
2/2	Контроль захищеності Wi-Fi.	Здійснювати контроль безпеки безпровідних мереж та застосовувати заходи по пошуку вразливостей мережевої інфраструктури.	Поточне опитування
2/-	Виявлення атак на безпровідні мережі	Виявляти та детектувати атаки на безпровідні мережі. Здійснювати аналіз мережевого трафіку.	Поточне опитування
2/-	Джерела даних для IDS/IPS	Використовувати засоби збору інформації про вразливі хости, встановлення та налаштування IDS/IPS систем.	Поточне опитування
2/-	Методи виявлення атак	Володіти основними методами та підходами виявлення атак, їхнього документування та опису.	Поточне опитування
2/-	Інтеграція засобів в єдину систему.	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	Поточне опитування

Рекомендовані джерела інформації

1. Опорний конспект лекцій з курсу «Моніторинг та управління інформаційною безпекою» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Укл.: Касянчук М.М., Івасьєв С.В. – Тернопіль: ЗУНУ, 2024. – 21 с.
2. Опорний конспект лекцій з курсу «Моніторинг та управління інформаційною безпекою» для здобувачів освітньо-професійної програми «Кібербезпека» другого (магістерського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Укл.: Касянчук М.М., Івасьєв С.В. – Тернопіль: ЗУНУ, 2024. – 21 с.
3. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
4. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.ISO 31010 2019. Risk management -Risk assessment techniques. Management du risque -Techniques. – 268 p.
5. Закон України «Про інформацію» URL: https://zakon.rada.gov.ua/laws/show/2657-12
6. Закон України Про захист інформації в інформаційнотелекомунікаційних системах № 80/94-ВР від 05.07.1994 р., URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
7. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». – Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с. 6. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. 482 p.
8. Яцків В.В., Івасьєв С.В., Давлетова А.Я., Тимошенко Л.М. Методологія впровадження системи управління інформаційною безпекою на основі багаторівневої моделі кіберзахисту згідно з вимогами законодавства України.- Інформатика та математичні методи в моделюванні Том 15, № 1, 2025, 137-149.
9. Управління інформаційною безпекою: навчально-методичний посібник./ А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с.
10. Bender David. Bender on Privacy and Data Protection. LexisNexis, 2020. - 2940 p.
11. Schreider Tari. Building an Effective Security Program. 2nd Edition. - Rothstein Associates Inc., 2020. - 406 p.

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами освіти і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу учасник може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими учасниками, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Оцінювання

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-6.	Підсумкове модульне тестування за темами №1-15.	Визначається як оцінка за звіт про виконання завдання тренінгу.	Підсумкове тестування за результатами опрацювання теоретичного матеріалу. Теоретичні питання: 25 питань по 4 бали - max 100 балів.	Теоретичні питання: 15 питань по 4 бали - max 60 балів. Практичне завдання - max 40 балів

Шкала оцінювання

За шкалою університуту	**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)