



Силабус курсу МОНІТОРИНГ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

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

Керівник курсу

ПП

Степан Івасьєв

Контактна інформація

s.ivasiev@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. Завданнями вивчення навчальної дисципліни є: реалізація захисту конфіденційності інформації; здійснення захисту цілісності інформації; сприяння доступності необхідної інформації. Завдання лекційних занять включає вивчення основних теоретичних понять та принципів, пов'язаних із моніторингом та управлінням інформаційною безпекою, а також аналіз сучасних викликів та стратегій в цій галузі. Завдання проведення практичних занять спрямоване на формування у студентів практичних навичок з моніторингу та управління інформаційною безпекою, включаючи вирішення реальних завдань та використання інструментів і методів для забезпечення безпеки даних та інформаційних систем.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Постановка задачі аналізу захищеності комп'ютерної системи. Методи виявлення вразливостей системи аналізу. Література, методичні рекомендації щодо дисципліни	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	Мережеві сканери безпеки. Способи збору інформації про мережу. Попереднє вивчення цілі	Володіння поняттями та вміння застосовувати сканування портів, сканування протоколів, прості методи визначення ОС, опитування стеку TCP/IP, інструменти SinFP. Використання протоколу ICMP, Port 0 OS Fingerprinting, активної ідентифікації ОС – перспективи.	Поточне опитування
2/0	Ідентифікація мережевих об'єктів. Визначення топології мережі	Навики використання протоколу ICMP, ідентифікації вузлів з допомогою протоколу ARP, відслідковування маршрутів і	Поточне опитування

		фільтрація, утиліти tracerproto.	
2/2	Ідентифікація статусу апорта, сервісів та додатків. Ідентифікація операційних систем.	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	Поточне опитування
2/0	Методи ідентифікації вразливостей по дотичних ознаках. Passive Fingerprinting.	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації	Поточне опитування
2/2	Виявлення вразливостей за допомогою тестів. Мережевий сканер Nessus	Розуміння понять експлоїт і їх різновидів. Вміння використання техніки запуску коду, віддаленого підбору паролів. Застосування оцінки стійкості паролів, тестування, можливостей сканера.	Поточне опитування
2/2	Мова опису атак NASL.	Розуміння структури сценарію., синтаксису мови і бібліотеки, які підключаються.	Поточне опитування
2/0	Сканери безпеки компанії Positive Technologies	Знання архітектури, основних можливостей, етапів роботи сканера XSpider. Вміння здійснювати збір інформації про мережу, ідентифікації вразливостей, локальні перевірки Windows, виявлення вразливостей web-додатків.	Поточне опитування
2/2	Аналіз захищеності на рівні вузла. Спеціалізовані засоби аналізу захищеності	Розуміти задачу локального сканування. Знання архітектури. Навики збору інформації і ідентифікації вразливостей. Класифікація сканерів безпеки по призначенню, загроз і вразливостей СУБД.	Поточне опитування
2/2	Методологія аналізу захищеності Ethical Hacking. Централізоване управління вразливостями	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
2/2	Контроль захищеності безпроводних мереж.	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	Поточне опитування
2/0	Виявлення атак на безпроводні мережі	Розуміти принципи моніторингу безпеки. Навики виявлення несанкціонованого використання безпроводних засобів, атаки на пристрої та і сервіси, атаки на механізми аутентифікації, атаки на клієнтів. Розуміти особливості виявлення атак та характерні атаки для безпроводних мереж.	Поточне опитування
2/0	Джерела даних для систем виявлення атак.	Розуміти складові технології виявлення атак. Аналізувати мережевий трафік як джерело даних.	Поточне опитування
2/0	Признаки атак. Методи виявлення атак	Виявляти атаки на рівні вузла. Аналізувати дані про потік. Вміння використовувати вразливості як ознаки атак. Ідентифікація	Поточне опитування

		відхилення від порогових значень.	
2/0	Інтеграція засобів виявлення і запобігання атак в єдину систему і взаємозв'язок з іншими засобами захисту.	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

Літературні джерела

1. Soni, Arun. The Cybersecurity Self-Help Guide. CRC Press, 2021.
2. Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 2021,13,39. <https://doi.org/10.3390/fi13020039>
3. ISO 31010 2019. Risk management -Risk assessment techniques. Management du risque -Techniques. – 268 p.
4. Wangen, G. Quantifying and Analyzing Information Security Risk from Incident Data; Graphical Models for Security; Albanese, M., Horne, R., Probst, C.W., Eds.; Springer International Publishing: Cham, Switzerland, 2019, pp. 129–154.
5. Radanliev P., et al. "Cyber Risk in IoT Systems." (2019).
6. Lee, In. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management." Future Internet 12.9, 2020: 157.
7. Шумейко О.О. Інформаційна безпека. Дніпровський державний технічний університет, 2019. - 155 с.
8. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
9. Мужанова Т.М. Інформаційна безпека держави. Київ: Державний університет телекомунікацій, 2019. - 131 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 дефлайнів 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: Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. 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 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне з оцінок, отриманих на практичних заняттях 1-5.	Підсумкова письмова робота за темами №1-15.	Оцінка за виконання одного завдання тренінгу	Оцінка за виконання одного завдання самостійної роботи	Теоретичні питання: 2 питання по 30 балів. Практичне завдання 40 балів

Шкала оцінювання:

За шкалою університету	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)