СИЛАБУС ДИСЦИПЛІНИ
«СИСТЕМИ МОНІТОРИНГУ ЗАГРОЗ ТА АТАК»

Ступінь вищої освіти – бакалавр
Спеціальність 125 – Кібербезпека
Освітня програма «Кібербезпека»
Рік навчання 4, семестр 7
Форма навчання денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор курсу	**Лахно Валерій Анатолійович, д.т.н., професор (портфоліо)** 
Контактна інформація лектора (e-mail)	**Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 0445278724 e-mail lva964@nubip.edu.ua**
Сторінка курсу в eLearn	**ЕНК (8 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=2773

ОПИС ДИСЦИПЛІНИ

Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області мережевої 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 систем та мереж.

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

У результаті вивчення даної навчальної дисципліни студент повинен:

Знати:

- види загроз інформації в комп’ютерних системах та мережах;
- основні протоколи безпеки;
- принципи функціонування систем захисту;
- основні програмні і апаратні засоби захисту інформації в комп’ютерних системах та мережах;
- засоби організації розмежування доступу комп’ютерних мережах.

Вміти:

- виконати аналіз безпеки комп'ютерної системи або мережі та усунути можливі шляхи несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконати адміністрування прав доступу до комп´ютерної системи та мережі з метою перешкоди призначення невиправданих привілеїв;
- перевірити надійність захисту інформації та стійкості його щодо хакерських атак шляхом моделювання загроз;
- підібрати тип та структуру локальної комп’ютерної мережі;
- підібрати комплекс необхідних апаратно-програмних засобів для захисту комп’ютерної системи та мережі.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Знання та розуміння предметної області та розуміння професії.

КЗ8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності:

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)..

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:

ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції, вебінари, щоб переконатися, що рухаєтесь за графіком навчання.

СТРУКТУРА КУРСУ

Тема	**Години** (лекції/ Лабораторні,)	Результати навчання	Завдання	Оцінювання
1 семестр				
Модуль 1. Моніторинг мережевої безпеки.				
Тема №1. Основніпоняття та концепції моніторингу. Компоненти тарівні систем моніторингу.	**2/0**	ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.	Опитування.	**-**
Тема №2. Побудова схеми управлінського моніторингу конкретного об'єкту	**2/4**		Захист лабораторної роботи.	**10**
Тема №3. Сутність моніторингу в окремих сферахдіяльності. Класифікація систем моніторингу.	**2/4**		Захист лабораторної роботи.	**10**
Тема №4. Функції, задачі та принципи організації моніторингу.	**2/2**		Опитування.	**2**
Тема №5. Датчики, як джерело збору інформації у автоматизованих системах моніторингу.	**2/2**		Опитування.	**2**
Тема №6. Дослідження принципів роботидатчиків.	**2/2**			
Модульний контроль			Підсумковий тест в ЕНК.	**30**
Модуль 2. Практичне застосування систем моніторингу загроз та атак.				
Тема № 7. Організація систем моніторингу загроз та атак підприємства.	**2/2**	ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-	Захист лабораторної роботи.	**10**
Тема №8. Системи моніторингу загроз підприємства АПК.	**2/0**		Опитування.	**-**

Тема № 9. Системи моніторингу комп'ютерних мереж, системи виявлення атак (СВА), сканери мережі SIEM, HP Operations Manager, ManageEngine OpManager, SolarWinds, IBM Tivoli, WhatsUp Gold.	**2/6**	телекомунікаційних системах. ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.	Опитування.	**2**
Тема № 10. Кібергігієна - як основа захисту відзагроз в інформаційному суспільстві.	**4/2**		Опитування.	**2**
Тема № 11. IDS.	**4/4**		Опитування.	**2**
Тема № 12. IPS.	**4/2**		Опитування.	**2**
Модульний контроль			Підсумковий тест в ЕНК.	**30**
Всього за семестр				**70**
Екзамен			**Тест, теоретичні питання, задача**	**30**
Всього за курс				**100**

ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів та перескладання:	Дедлайни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження).
Політика щодо академічної доброчесності:	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
Політика щодо відвідування:	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету).

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзаменів	**Заліків**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Рекомендовані джерела інформації

1. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

2. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с.

3. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.

4. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ "ПоліграфКонсалтинг", 2010. – 216 с.

5. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.