СИЛАБУС ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І КІБЕРБЕЗПЕКА»
ЧАСТИНА 1

Ступінь вищої освіти – Магістр
Спеціальність 123 – КОМП'ЮТЕРНА ІНЖЕНЕРІЯ
Освітня програма «Комп'ютерні системи і мережі»
Рік навчання 1, семестр 1
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 (1 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=1886

ОПИС ДИСЦИПЛІНИ

Навчальна дисципліна передбачає вивчення теоретичних основ проблеми зберігання, передачі, перетворення, закриття та відновлення інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності, способів захисту від несанкціонованого доступу до інформації. Вивчаються методологічні, організаційні та наукові основи розробки апаратно-програмних засобів і систем збору та захисту інформації (ЗІ), забезпечення інформаційної безпеки процесів опрацювання, зберігання та поширення інформації в інформаційно-комунікаційних мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем і засобів здійснення погроз з боку потенційних порушників.

Навчальна дисципліна забезпечує формування ряду загальних та фахових компетентностей:

ЗК1. Здатність до адаптації та дій в новій ситуації.

ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.

ЗК7. Здатність приймати обґрунтовані рішення.

СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

СК8. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.

СК9. Здатність представляти результати власних досліджень та/або розробок у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.

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

ПРН3. Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.

Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від теоретичного та практичного

матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції на ЕНК, вебінари, щоб переконатися, що рухаєтесь за графіком навчання.

СТРУКТУРА КУРСУ

Тема	Години (лекції/ Лаб.)	Результати навчання	Завдання	Оцінювання
1 семестр				
Модуль 1. Механізми реалізації послуг безпеки.				
Тема 1. Властивості інформації з точки зору проблематики її захисту.	**2/0**	Вміти застосовувати теоретичні знання та практичні навички для розв'язування задач аналізу та синтезу захищених ІКС, КМ та IoT систем, зокрема, для агропромислового комплексу країни.	Опитування.	
Тема 2. Ризики порушення політики інформаційної безпеки. Вимоги щодо безпеки системи, ризики безпеки.	**3/4**	Вміти здійснювати формалізований опис політик інформаційної безпеки для об'єктів захисту.	Захист лабораторної роботи.	**10**
Тема 3. Механізми реалізації послуг безпеки.	**4/4**	Вміти розробляти програмне забезпечення для систем захисту інформації та IoT систем, мобільних систем, використовуючи сучасні технології програмування. Вміти аналізувати ПЗ з точки зору безпеки його використовування в ІКС.	Захист лабораторної роботи.	**10**
Тема 4. Поняття загрози інформації.	**2/4**	Вміти розробляти моделі загроз та порушника. Вміти здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.	Захист лабораторної роботи.	**10**
Тема 5. Політика інформаційної безпеки. Аналіз моделей безпеки ІКС. Загальні моделі ІБ.	**2/2**	Вміти забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	Захист лабораторної роботи.	**10**
Тема 6. Аналіз безпеки програмного забезпечення.	**3/2**	Вміти забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.	Захист лабораторної роботи.	**10**
Модульний контроль			Підсумковий тест в ЕНК	**30**
Модуль 2. Моделювання та аналіз безпеки об'єктів кіберзахисту.				
Тема 7. Модель архітектури безпеки ІКС.	**2/2**	Вміти забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.	Захист лабораторної роботи.	**10**

Тема 8. Методи захисту інформації в ІКС.	**2/2**	Вміти застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.	Захист лабораторної роботи.	**10**
Тема 9. Задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.	**2/2**	Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки	Захист лабораторної роботи.	**10**
Тема 10. Криптографічний захист інформації (Ч1).	**4/4**	Вміти вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.	Захист лабораторної роботи.	**10**
Тема 11. Криптографічний захист інформації (Ч1).	**4/4**	Вміти вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.	Захист лабораторної роботи.	**10**
Модульний контроль			Підсумковий тест в ЕНК.	**30**
Всього за 1 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