СИЛАБУС ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І КІБЕРБЕЗПЕКА»
Частина 2

Ступінь вищої освіти – Магістр
Спеціальність 123 – КОМП'ЮТЕРНА ІНЖЕНЕРІЯ
Освітня програма «Комп'ютерні системи і мережі»
Рік навчання 1, семестр 2
Форма навчання денна
Кількість кредитів ЄКТС 6
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
2 семестр				
Модуль 1. Захист у технічних каналах витоку інформації.				
Тема 1. Концептуальні засади забезпечення інформаційної безпеки (ІБ) України.	**2/0**	Вміти аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	Опитування.	**5**
Тема 2. Доктрина ІБ України.	**2/0**	Вміти діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.	Опитування.	**5**
Тема 3. Технічні канали витоку інформації.	**2/0**	Вміти вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації, зокрема для галузі АПК.	Опитування.	**5**
Тема 4. Способи несанкціонованого зняття інформації.	**2/6**	Здатність застосовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	Здача лабораторної роботи.	**10**
Тема 5. Методи та засоби блокування технічних каналів витоку інформації.	**2/6**	Вміти вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації, зокрема для галузі АПК.	Здача лабораторної роботи.	**10**
Тема 6. Методи та засоби захисту електромагнітної інформації.	**2/6**	Вміти вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	Здача лабораторної роботи.	**10**
Тема 7. Методи захисту інформації у автоматизованих системах (АС) (Частина 1).	**2/6**	Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем, вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	Здача лабораторної роботи.	**10**

Тема 8. Методи захисту інформації у АС (Частина 2).	**2/6**	Вміти аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.	Здача лабораторної роботи.	**10**
Тема 9. Методи захисту інформації у телекомунікаційних мережах та відкритих мережах зв'язку.	**4/0**	Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.	Опитування	**5**
Модульний контроль			Підсумковий тест в ЕНК	**30**
Модуль 2. Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем.				
Тема 10. Загальні принципи побудови захищених інформаційно-комунікаційних систем (ЗІКС) та КМ.	**4/6**	Знати загальні принципи побудови захищених інформаційно-комунікаційних систем (ЗІКС) та комп'ютерних мереж (КМ).	Здача лабораторної роботи.	**10**
Тема 11. Основні принципи організації взаємодії в ЗІКС та КМ.	**4/6**	Вміти приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.	Здача лабораторної роботи.	**10**
Тема 12. Програмне забезпечення для адміністрування ЗІКС та КМ.	**4/6**	Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	Здача лабораторної роботи.	**10**
Тема 13. Якісний та кількісний аналіз ризику для ІБ та КБ об'єкту інформатизації.	**4/6**	Вміти вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	Здача лабораторної роботи.	**10**
Тема 14. Методи кількісної оцінки ступеня ризику: аналітичний метод; метод використання аналогів. Комплексна оцінка ризиків для ІБ.	**4/6**	Вміти вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.	Здача лабораторної роботи. Неформальна on-line освіта на основі МВОК.	**10** **20**
Модульний контроль			Підсумковий тест в ЕНК	**30**
Всього за 2 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