



**СИЛАБУС ДИСЦИПЛІНИ  
«ТЕХНОЛОГІЇ ПОБУДОВИ ЗАХИЩЕНИХ  
КОМП'ЮТЕРНИХ СИСТЕМ»  
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](mailto:lva964@nubip.edu.ua)

Сторінка курсу в eLearn

ЕНК (2 семестр) <https://elearn.nubip.edu.ua/course/view.php?id=2945>

### 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.

**Інтегральна компетентність** - здатність розв'язувати складні задачі і проблеми в галузі комп'ютерної інженерії або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

**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 набере певні програмні результати, а саме**

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

ПРН5. Розробляти і реалізовувати проекти у сфері комп'ютерної інженерії та дотичні до неї міждисциплінарні проекти з урахуванням інженерних, соціальних, економічних, правових та інших аспектів.

**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	Годин и (лекції/ Лаб.)	Результати навчання	Завдання	Оцінювання
<b>2 семестр</b>				
<b>Модуль 1. Захист у технічних каналах витоку інформації.</b>				
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 заводових 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 в КС.	2/6	Вміти вимірювати параметри небезпечних та заводових 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	2/6	Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту	Здача лабораторної роботи.	10

системах (АС) (Частина 1).		інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем, вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.		
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
<b>Модуль 2. Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем.</b>				
Тема 10. Загальні принципи побудови захищених КС 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 захищених КС 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 захищених КС 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
<b>Всього за 2 семестр</b>				<b>70</b>
<b>Екзамен</b>			<b>Тест, теоретичні питання, задача</b>	<b>30</b>
<b>Всього за курс</b>				<b>100</b>

## ПОЛІТИКА ОЦІНЮВАННЯ

<b>Політика щодо дедлайнів та перескладання:</b>	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).
<b>Політика щодо академічної доброчесності:</b>	Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
<b>Політика щодо відвідування:</b>	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. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с
2. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсєєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.
3. Браїловський М.М. Захист інформації у банківській діяльності / М.М. Браїловський, Г.П. Лазарев, В.О. Хорошко. – К.: ТОВ “ПоліграфКонсалтинг”, 2010. – 216 с.
4. Проектування 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.
5. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.).
6. Сагун А.В., Лахно В.А., Бобков В.Б., Касаткін Д.Ю., Хайдуров В.В. навчальний посібник «Спеціалізовані комп'ютери» / А.В.Сагун, В.А.Лахно, В.Б.Бобков, Д.Ю.Касаткін, В.В.Хайдуров // НУБіП України, - Київ, Видавничий центр Компринт 2021, 24 у.д.а.
7. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.