

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**
Кафедра комп'ютерних систем, мереж та кібербезпеки

“ЗАТВЕРДЖУЮ”

**Декан факультету інформаційних
технологій**

_____ проф. Ігор БОЛБОТ
“ 02 ” _____ 06 _____ 2025 р.

“СХВАЛЕНО”

на засіданні кафедри
комп'ютерних систем,
мереж та кібербезпеки

Протокол № 09 від 26.05.2025 р.

Завідувач кафедри

_____ Дмитро КАСАТКІН

”РОЗГЛЯНУТО ”

Гарант ОП «Комп'ютерні системи і
мережі»

_____ Вадим ШКАРУПИЛО

**РОБОЧА ПРОГРАМА
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**
“ТЕХНОЛОГІЇ ПОБУДОВИ ЗАХИЩЕНИХ КОМП'ЮТЕРНИХ СИСТЕМ
(Частина 1)”

Галузь знань F – Інформаційні технології

Спеціальність F7 – «Комп'ютерна інженерія»

Освітня програма «Комп'ютерні системи і мережі»

Факультет (ННІ) Інформаційних технологій

Розробник: професор, д.т.н., професор Лахно В.А.

Київ – 2025 р.

Опис навчальної дисципліни
Технології побудови захищених комп'ютерних систем (Частина 1)
(назва)

Дисципліна "Технології побудови захищених комп'ютерних систем" націлена на вивчення сучасних методів та технологій для створення та підтримки безпечних комп'ютерних систем. Курс орієнтований на підготовку фахівців, здатних проектувати, впроваджувати та забезпечувати безпеку інфраструктури інформаційних систем. Студенти ознайомлюються з основними принципами захисту інформації, вивчають використання криптографічних протоколів, механізмів аутентифікації та авторизації, а також методи моніторингу й виявлення вторгнень і управління ризиками. Протягом курсу студенти освоюють передові технології та міжнародні стандарти кібербезпеки, а також набувають практичних навичок у захисті комп'ютерних мереж, серверних та клієнтських додатків, баз даних і хмарних платформ.

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Освітній ступінь	магістр	
Галузь знань	F – Інформаційні технології	
Спеціальність	F7 – «Комп’ютерна інженерія»	
Освітня програма	Комп’ютерні системи і мережі	
Характеристика навчальної дисципліни		
Вид	Обов’язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2025-2026	
Семестр	1	
Лекційні заняття	30 год.	
Практичні, семінарські заняття		
Лабораторні заняття	30 год.	
Самостійна робота	60 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	10 (5 тижнів)	

1. Мета та завдання навчальної дисципліни

Мета - є вивчення теоретичних основ проблеми зберігання, опрацювання, пошуку, передачі, перетворення, закриття та відновлення конфіденційної інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності, способів захисту від несанкціонованого доступу до інформації в сучасних комп'ютерних системах (КС). Вивчення методологічних, організаційних та наукових основ розробки 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 набуде певні програмні результати, а саме

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

2. Програма та структура навчальної дисципліни для:

– повного терміну денної (заочної) форми навчання

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Модуль 1. Політика інформаційної безпеки КС.												
Тема 1. Властивості інформації з точки зору проблематики її захисту в комп'ютерних системах.	7	2		-		5						
Тема 2. Ризики порушення політики інформаційної безпеки. Вимоги щодо кібербезпеки КС.	12	3		4		5						
Тема 3. Механізми реалізації послуг безпеки КС.	13	4		4		5						
Тема 4. Поняття загрози інформації.	11	2		4		5						
Тема 5. Політика інформаційної безпеки. Аналіз моделей безпеки КС. Загальні моделі ІБ.	9	2		2		5						
Тема 6. Аналіз безпеки програмного забезпечення КС.	10	3		2		5						
Разом за змістовим модулем 1	62	16		16		30						
Модуль 2. Моделювання та аналіз безпеки об'єктів кіберзахисту.												
Тема 7. Модель архітектури безпеки КС.	10	2		2		6						

Тема 8. Методи захисту інформації в КС.	10	2		2		6						
Тема 9. Задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в КС згідно встановленої політики ІБ.	10	2		2		6						
Тема 10. Криптографічний захист інформації (Ч1).	14	4		4		6						
Тема 11. Криптографічний захист інформації (Ч2).	14	4		4		6						
Разом за змістовим модулем 2	58	14		14		30						
Усього годин за курс	120	30		30		60						

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Властивості інформації з точки зору проблематики її захисту в комп'ютерних системах.	2
2	Ризики порушення політики інформаційної безпеки. Вимоги щодо кібербезпеки КС.	3
3	Механізми реалізації послуг безпеки КС.	4
4	Поняття загрози інформації.	2
5	Політика інформаційної безпеки. Аналіз моделей безпеки КС.	2
6	Аналіз безпеки програмного забезпечення КС.	3
7	Модель архітектури безпеки КС.	2
8	Методи захисту інформації в КС.	2
9	Задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в КС згідно встановленої політики ІБ.	2
10	Криптографічний захист інформації (Ч1).	4
11	Криптографічний захист інформації (Ч2).	4
	Разом	30

4. Теми лабораторних (практичних, семінарських) занять

№ з/п	Назва теми	Кількість годин
1	Аналіз ризиків порушення політики інформаційної безпеки КС.	4
2	Планування заходів щодо впровадження механізмів реалізації послуг безпеки.	4
3	Аналіз моделей безпеки КС для КС.	4
4	Аналіз безпеки програмного забезпечення для КС.	2
5	Побудова концептуальної моделі архітектури безпеки КС КС.	2
6	Планування методів захисту інформації в КС.	2
7	Автентифікація користувачів у КС.	4
8	Застосування криптографічного захисту інформації у КС.	4
9	Методи криптоаналізу.	4
	Разом	30

4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Властивості інформації з точки зору проблематики її захисту та кібербезпеки об'єкту інформатизації (ОБІ).	5

2	Ризики порушення політики інформаційної безпеки ОБІ.	5
3	Сучасні вимоги щодо безпеки системи, ризики безпеки ОБІ.	5
4	Механізми реалізації послуг безпеки ОБІ.	5
5	Політика інформаційної безпеки ІКС або ОБІ. Поняття загрози інформації.	5
6	Моделі безпеки ІКС.	5
7	Проблематика безпеки програмного забезпечення.	6
8	Модель архітектури безпеки ІКС.	6
9	Інноваційні методи захисту інформації в ІКС.	6
10	Автентифікація користувачів на ОБІ та у ІКС підприємств.	6
11	Криптографічний захист інформації. Криптографічні протоколи.	6
	Разом	60

5. Засоби діагностики результатів навчання:

- екзамен;
- модульні тести;
- захист та лабораторних робіт.

6. Методи навчання:

- словесний метод (лекція, дискусія, співбесіда тощо);
- практичний метод;
- наочний метод (метод ілюстрацій, метод демонстрацій);
- робота з навчально-методичною літературою;
- відеометод (дистанційні, мультимедійні, веб-орієнтовані тощо);
- самостійна робота (виконання завдань).

7. Методи оцінювання.

(вибрати необхідне чи доповнити)

- екзамен;
- захист практичних робіт;
- презентації та виступи на наукових заходах.

8. Оцінювання результатів навчання.

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України»

8.1. Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Модуль 1. Політика інформаційної безпеки КС.		
Лекція 1		-
Лабораторна/практична робота 1.		-
Самостійна робота 1.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Лекція 2		-

Лабораторна/ практична робота 2.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 2.	-	10
Лекція 3	-	-
Лабораторна/практич на робота 3.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 3.	-	10
Лекція 4	-	-
Лабораторна/ практична робота 4.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 4.	-	10
Лекція 5	-	-
Лабораторна/ практична робота 5.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота	-	5
Лекція 6	-	-
Лабораторна/практич на робота 6.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 6.	-	5
Модульна контрольна робота 1.		30
Всього за модулем 1		100
Модуль 2. Моделювання та аналіз безпеки об'єктів кіберзахисту.		
Лекція 7	-	-
Лабораторна/ практична робота 7.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 7.	-	10
Лекція 8	-	-
Лабораторна/ практична робота 8.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 8.	-	10
Лекція 9	-	-
Лабораторна/ практична робота 9.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 9.	-	10
Лекція 10	-	-
Лабораторна/ практична робота 10.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 10.	-	10
Лекція 11	-	-
Лабораторна/ практична робота 11.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	5
Самостійна робота 11.	-	5
Модульна контрольна робота 2.	-	30
Всього за модулем 2		100
Навчальна робота	$(M1 + M2)/2 \cdot 0,7 \leq 70$	
Екзамен/залік	30	
Всього за курс	$(\text{Навчальна робота} + \text{екзамен}) \leq 100$	

8.2. Шкала оцінювання знань здобувача вищої освіти

Рейтинг здобувача вищої освіти, бали	Оцінка за національною системою (екзамени/заліки)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

8.3. Політика оцінювання

Політика щодо дедлайнів та перескладання	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).
Політика щодо академічної доброчесності	Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Реферати повинні мати коректні текстові посилання на використану літературу
Політика щодо відвідування	Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в он-лайн формі за погодженням із деканом факультету)

9. Навчально-методичне забезпечення

Електронний навчальний курс (<https://elearn.nubip.edu.ua/course/view.php?id=4571>) на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

10. Рекомендовані джерела інформації

Базова

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. Технічний захист інформації: Навч. погіб. в 2 ч. Ч. 1: Основи технічного захисту інформації / В.М.Богущ, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2022. - 286с.
8. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.

Допоміжна

1. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах [Електронний ресурс] : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак ; КПП ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,73 Мбайт). – Київ : КПП ім. Ігоря Сікорського, 2020. – 78 с.