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 2)"

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 2)

(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»	
Характеристика навчальної дисципліни		
Вид	Обов'язкова	
Загальна кількість годин	180	
Кількість кредитів ECTS	6	
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	2	
Лекційні заняття	40 год.	
Практичні, семінарські заняття		
Лабораторні заняття	60 год.	
Самостійна робота	80 год.	
Курсовий проект (робота)	+	
Кількість тижневих годин для денної форми навчання: аудиторних	20 (10 тижнів)	

1. Мета та завдання навчальної дисципліни

Мета - є формування у майбутніх фахівців умінь та компетенцій для забезпечення ефективного захисту інформації у комп'ютерних системах (КС), необхідних для подальшої роботи за фахом комп'ютерна інженерія та навчити їх застосуванню методів, технологій та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій на зростання кількості та складності деструктивних впливів на інформаційні ресурси установ та підприємств.

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. Захист у технічних каналах витоку інформації.												
Тема 1. Концептуальні засади забезпечення кібербезпеки (КБ) України.	6	2		-		4						
Тема 2. Доктрина КБ України.	8	2		-		6						
Тема 3. Технічні канали витоку інформації.	8	2		-		6						
Тема 4. Способи несанкціонованого зняття інформації.	12	2		6		4						
Тема 5. Методи та засоби блокування технічних каналів витоку інформації в КС.	12	2		6		4						
Тема 6. Методи та засоби захисту електромагнітної інформації.	12	2		6		4						
Тема 7. Методи захисту інформації у автоматизованих системах (АС) (Частина 1).	12	2		6		4						
Тема 8. Методи захисту інформації у АС (Частина 2).	12	2		6		4						
Тема 9. Методи захисту інформації у телекомунікаційних мережах та відкритих мережах зв'язку.	8	4		-		4						
Разом за змістовим модулем 1	**90**	**20**		**30**		**40**						
Модуль 2. Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем.												
Тема 10. Загальні принципи побудови захищених КС та КМ.	10	4		6		8						
Тема 11. Основні принципи організації взаємодії в захищених КС та КМ.	10	4		6		8						

Тема 12. Програмне забезпечення для адміністрування захищених КС та КМ.	10	4		6		8						
Тема 13. Якісний та кількісний аналіз ризику для КБ об'єкту інформатизації.	14	4		6		8						
Тема 14. Методи кількісної оцінки ступеня ризику: аналітичний метод; метод використання аналогів. Комплексна оцінка ризиків для КБ.	14	4		6		8						
Разом за змістовим модулем 2	**90**	**20**		**30**		**40**						
Усього годин за курс	**180**	**40**		**60**		**80**						

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Концептуальні засади забезпечення кібербезпеки (КБ) України.	2
2	Доктрина КБ України.	2
3	Технічні канали витоку інформації.	2
4	Способи несанкціонованого зняття інформації.	2
5	Методи та засоби блокування технічних каналів витоку інформації в КС.	2
6	Методи та засоби захисту електромагнітної інформації.	2
7	Методи захисту інформації у автоматизованих системах (АС) (Частина 1).	2
8	Методи захисту інформації у АС (Частина 2).	2
9	Методи захисту інформації у телекомунікаційних мережах та відкритих мережах зв'язку.	4
10	Загальні принципи побудови захищених КС та КМ.	4
11	Основні принципи організації взаємодії в захищених КС та КМ.	4
12	Програмне забезпечення для адміністрування захищених КС та КМ.	4
13	Якісний та кількісний аналіз ризику для КБ об'єкту інформатизації.	4
14	Методи кількісної оцінки ступеня ризику: аналітичний метод; метод використання аналогів. Комплексна оцінка ризиків для КБ.	4
	Разом	**40**

4. Теми лабораторних (практичних, семінарських) занять

№ з/п	Назва теми	Кількість годин
1	Способи несанкціонованого зняття інформації.	6
2	Засоби блокування технічних каналів витоку інформації в КС.	6
3	Засоби захисту електромагнітної інформації.	6
4	Аналіз методів захисту інформації у автоматизованих системах.	6
5	Адміністрування та експлуатація захищених інформаційно-комунікаційних систем.	6
6	Програмне забезпечення для адміністрування ЗІКС та КМ.	6
7	Адміністрування у ОС NetWare фірми Novell.	6
8	Якісний та кількісний аналіз ризику для ІБ та КБ об'єкту інформатизації (ОБІ).	6
9	Аналізу ступеня ризику для КБ ОБІ.	6
10	Кількісна оцінка ступеня ризику для КБ.	6
	Разом	**60**

5. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Технічні канали витоку інформації та механізм їх утворення.	4
2	Методи та засоби захисту електромагнітної інформації.	6
3	Методи захисту інформації у автоматизованих системах.	6
4	Адміністрування та експлуатація захищених інформаційно-комунікаційних систем.	4
5	Програмне забезпечення для адміністрування ЗІКС та КМ.	4
6	Адміністрування у ОС NetWare фірми Novell.	4
7	Засоби управління локальними ресурсами ЗІКС та КМ.	4
8	Якісний та кількісний аналіз ризику для ІБ та КБ об'єкту інформатизації (ОБІ).	4
9	Визначення ступеня ризику для ІБ ОБІ.	4
10	Кількісна оцінка ступеня ризику для ІБ.	8
11	Система управління ризиками ІБ.	8
12	Комплексне управління довгостроковими інвестиціями у політику ІБ ОБІ.	8
13	Комплексна оцінка ризиків для КБ.	8
14	Оптимізація складу засобів КБ.	8
	Разом	**80**

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. Захист у технічних каналах витоку інформації.		
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.	-	-
Лекція 3	-	-
Лабораторна/практична робота 3.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	**5**
Самостійна робота 3.	-	-
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.	-	**5**
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/практична робота 6.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	**5**
Самостійна робота 6.	-	**5**
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.	-	**5**
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.	-	**5**
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.	-	-
Модульна контрольна робота 1.		**30**
Всього за модулем 1		**100**
Модуль 2. Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем.		
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.	-	**10**

Лекція 12	-	**-**
Лабораторна/ практична робота 12.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	**5**
Самостійна робота 12.		**10**
Лекція 13		**-**
Лабораторна/ практична робота 13.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	**5**
Самостійна робота 13.	-	**10**
Лекція 14	-	**-**
Лабораторна/ практична робота 14.	Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.	**5**
Самостійна робота 14.	-	**5**
Модульна контрольна робота 2.		**30**
Всього за модулем 2		**100**
Навчальна робота		**(М1 + М2)/2*0,7 ≤ 70**
Екзамен/залік	**30**	
Всього за курс		**(Навчальна робота + екзамен) ≤ 100**
Курсовий проект/робота		**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=2945) на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт.

10. Рекомендовані джерела інформації

Базова

1. 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.

2. 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.

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

4. 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.

5. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, 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.Богуш, 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 ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,73 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 78 с.