Форма № Н - 3.04

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

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
проф. О.І. Глазунова
"___" _____ 2023 р.

"СХВАЛЕНО"
на засіданні кафедри
комп'ютерних систем,
мереж та кібербезпеки
Протокол №10 від 17.05.2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

"РОЗГЛЯНУТО"
Гарант ОП «Комп'ютерні системи і мережі»
(Шкарупило В.В.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "ТЕХНОЛОГІЇ ПОБУДОВИ ЗАХИЩЕНИХ КОМП'ЮТЕРНИХ СИСТЕМ (Частина 2)"

зі спеціальності 123 – «Комп'ютерна інженерія»
(шифр і назва напряму підготовки)
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Комп'ютерні системи і мережі»

факультет інформаційних технологій
(назва факультету)

Київ – 2023 р.

1. Опис навчальної дисципліни

Технології побудови захищених комп'ютерних систем (Частина 2)

(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	123 – «Комп'ютерна інженерія»	
другий (магістерський) рівень	Магістр	
Характеристика навчальної дисципліни		
Вид	Обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	6	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2023-2024	
Семестр	2	
Лекційні заняття	40 год.	
Практичні, семінарські заняття		
Лабораторні заняття	60 год.	
Самостійна робота	80 год.	
Індивідуальні завдання		
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.

Завдання навчальної дисципліни «Технології побудови захищених комп'ютерних систем (Частина 2)» - є теоретичне та практичне засвоєння необхідного рівня умінь та компетенцій, необхідних для подальшої роботи в умовах зростаючої інформатизації суспільства та підвищення рівня загроз інформаційній та кібербезпеці безпеці.

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.

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

3. 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
Змістовий модуль 1. Захист у технічних каналах витоку інформації.												
Тема 1. Концептуальні засади забезпечення інформаційної безпеки (ІБ) України.	6	2		-		4						
Тема 2. Доктрина ІБ 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**						

Змістовий 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 ІБ та КБ об'єкту інформатизації.	14	4		6		8						
Тема 14. Методи кількісної оцінки ступеня ризику: аналітичний метод; метод використання аналогів. Комплексна оцінка ризиків для ІБ.	14	4		6		8						
Разом за змістовим модулем 2	**90**	**20**		**30**		**40**						
Усього годин за курс	**180**	**40**		**60**		**80**						

4. Теми лабораторних занять

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

5. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Технічні канали витоку інформації та механізм їх утворення.	6
2	Методи та засоби захисту електромагнітної інформації.	4
3	Методи захисту інформації у автоматизованих системах.	4
4	Адміністрування та експлуатація захищених інформаційно-комунікаційних систем.	6
5	Програмне забезпечення для адміністрування ЗІКС та КМ.	6

6	Адміністрування у ОС NetWare фірми Novell.	6
7	Засоби управління локальними ресурсами ЗІКС та КМ.	10
8	Якісний та кількісний аналіз ризику для ІБ та КБ об'єкту інформатизації (ОБІ).	4
9	Визначення ступеня ризику для ІБ ОБІ.	6
10	Кількісна оцінка ступеня ризику для ІБ.	8
11	Система управління ризиками ІБ.	10
12	Комплексне управління довгостроковими інвестиціями у політику ІБ ОБІ.	10
	Разом	**80**

6. Методи навчання

Проведення лекцій з використанням технічних засобів навчання. Проведення лабораторних робіт та самостійної роботи засобами інформаційно-комунікаційних технологій в освіті. Використовується електронний навчальний курс на платформі Moodle «Технології побудови захищених комп'ютерних систем (Частина 2)».

7. Форми контролю

Наприкінці кожного змістовного модуля проводиться контрольна робота у вигляді тесту, що створений у комп'ютерному навчальному середовищі. Підсумкова атестація: іспит.

8. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

Оцінка виконання та захисту лабораторних робіт за кожний модуль здійснюється у наступній відповідності:

№ лабораторної роботи	**Кількість балів**	**Загальна кількість балів**
1 модуль		
Лабораторна робота № 1	10	70
Лабораторна робота № 2	10	
Лабораторна робота № 3	10	
Лабораторна робота № 4	10	
Лабораторна робота № 5	10	
Самостійна робота	20	
Модульна контрольна		30
2 модуль		
Лабораторна робота № 6	10	70
Лабораторна робота № 7	10	
Лабораторна робота № 8	10	

Лабораторна робота № 9	10	
Лабораторна робота № 10	10	
Самостійна робота	20	
Модульна контрольна		30

9. Методичне забезпечення

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

10. Рекомендована література

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. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.
8. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.

Допоміжна

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S., ... & Florov, S. (2021). Synergy of building cybersecurity systems.