НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Кафедра комп'ютерних наук

«ЗАТВЕРДЖЕНО»
Факультет інформаційних технологій
"12" червня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології захисту інформації

Галузь знань	Інформаційні технології
Спеціальність	Комп'ютерні науки
Освітня програма	Комп'ютерні науки
Факультет (ННІ)	Інформаційних технологій
Розробники:	доцент, к.т.н., доцент Пархоменко І.І.
	(посада, науковий ступінь, вчене звання)

КИЇВ 2025

Опис навчальної дисципліни _____Комп'ютерні науки_____

Дисципліна «Технології захисту інформації» є вибірковою дисципліною і входить в професійний цикл, який формує базовий рівень знань для освоєння загально-професійних навичок. Навчальною задачею дисципліни "Технології захисту інформації" є вивчення теоретичних основ, методології та принципів застосування технологій захисту інформації в комп'ютерних системах та мережах.

Дисципліни, які мають передувати вивченню курсу «Технології захисту інформації»:

1) «Основи програмної інженерії»
2) «Інформаційні технології»;
3) «Комп'ютерні мережі».
4) Операційні системи

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*бакалавр*	
Спеціальність	*122 "Комп'ютерні науки"*	
Освітня програма	*Комп'ютерні науки*	
Характеристика навчальної дисципліни		
Вид	*вибіркова*	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (за наявності)	-	
Форма контролю	*екзамен*	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	4	
Семестр	7	
Лекційні заняття	*15 год.*	- *год.*
Практичні, семінарські заняття	- *год.*	- *год.*
Лабораторні заняття	*15 год.*	- *год.*
Самостійна робота	*90 год.*	- *год.*
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	*2 год.*	

1. Мета, компетентності та програмні результати навчальної дисципліни

Метою дисципліни "*Технології захисту інформації*" - формування теоретичних знань та практичних навичок з організації та функціонування сучасних програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах та протидії сторонньому кібернетичному впливу в умовах неповноти та невизначеності.

Завдання дисципліни – забезпечити здатність студентів розуміти і застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

У результаті вивчення навчальної дисципліни студент повинен:

знати:

- основні положення теорії захисту інформації та кібербезпеки;
- канали витоку інформації, захист інформації від соціотехнічних атак;
- технології та основні шляхи забезпечення захисту інформації, в тому числі і в комп'ютерних мережах;
- основні напрямки розвитку сучасної криптографії та принципи криптоаналізу;
- шляхи захисту інформації в персональних комп'ютерах та комп'ютерних мережах;
- системи шифрування даних, які передаються в мережах;
- принципи безпечного проектування програмного забезпечення;
- принципи функціонування вбудованих засобів захисту комп'ютерних систем;
- принципи функціонування систем захисту, призначення привілей, зберігання паролів та автентифікація користувачів в операційних системах;
- методи побудови захисту окремих програмних продуктів;
- основні прийоми і програмні засоби для аналізу та дизасемблювання програмних продуктів з метою їх подальшого несанкціонованого використання.

вміти:

- виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконувати адміністрування прав доступу до комп'ютерної системи з метою перешкоди призначення невиправданих привілей;
- виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації;
- використовувати основні прийоми та програмні засоби хакерів для перевірки надійності захисту інформації та стійкості його щодо хакерських атак.
- застосовувати на практиці підходи для забезпечення кібербезпеки та захист інформації від кібератак
- застосовувати механізми захисту операційних систем об'єктів інформаційної діяльності та об'єктів критичної інформаційної інфраструктури
- застосовувати засоби управління, збереження і доступу до паролів та правила роботи з ними, механізми захисту операційних систем
- застосовувати засоби автентифікації користувачів і аналізу безпеки систем
- вживати заходи щодо забезпечення безпеки комп'ютерних мереж в умовах неповноти та невизначеності вхідних даних

2. Програма та структура навчальної дисципліни

Назви змістових модулів і тем	**Кількість годин**												
	денна форма							**заочна форма**					
	тижні	усього	у тому числі					усього	у тому числі				
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
Модуль 1. Основні положення теорії захисту інформації та кібербезпека													
Тема 1. Технології та основні шляхи забезпечення захисту інформації	1-2	24	2		2		20						

Назви змістових модулів і тем	Кількість годин													
	денна форма							заочна форма						
	тижні	усього	у тому числі					усього	у тому числі					
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.	
Тема 2. Канали витоку інформації. Захист інформації від соціотехнічних атак.	3-6	24	2		2		20							
Тема 3. Захист інформації на персональних комп'ютерах. Засоби мережевого захисту інформації. Моделі захисту.	7-8	26	3		3		20							
Разом за модулем 1		**74**	**7**		**7**		**60**							
Модуль 2. Методи та засоби забезпечення захисту інформації														
Тема 4. Основні напрямки розвитку сучасної криптографії та принципи криптоаналізу	9-10	28	4		4		20							
Тема 5. Паролі і механізми контролю за доступом. Протоколи автентифікації. Брандмауери	11 -13	24	2		2		20							
Тема 6. Методи та засоби забезпечення захисту інформації та безпечного проектування програмного забезпечення	14 -15	24	2		2		20							
Разом за модулем 2		**76**	**8**		**8**		**60**							
Усього годин		**150**	**15**		**15**		**120**							

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Основні положення теорії захисту інформації та кібербезпека. Технології та основні шляхи забезпечення захисту інформації.	1
2	Канали витоку інформації. Захист інформації від соціотехнічних атак.	2
3	Захист інформації на персональних комп'ютерах.	2
4	Засоби мережевого захисту інформації. Моделі захисту	2
5	Основні напрямки розвитку сучасної криптографії та принципи криптоаналізу.	2
6	Системи шифрування даних, які передаються в мережах. Цифрові підписи. Механізми та протоколи керування ключами в (PKI) інформаційної системи	2
7	Паролі і механізми контролю за доступом. Протоколи автентифікації. Брандмауери.	2
8	Методи та засоби забезпечення захисту інформації та безпечного проектування програмного забезпечення	2
Разом		**15**

4. **Теми лабораторних занять**

№ з/п	Назва теми	Кількість годин
1	Дослідження підходів для забезпечення кібербезпеки та захист інформації від кібератак	1
2	Дослідження механізмів захисту об’єктів інформаційної діяльності та об’єктів критичної інформаційної інфраструктури	2
3	Дослідження застосовування засобів управління, збереження і доступу до паролів та правила роботи з ними, механізмів захисту операційних систем	2
4	Дослідження застосування засобів автентифікації користувачів і аналіз безпеки систем	2
5	Дослідження засобів забезпечення безпеки комп’ютерних мереж	2
6	Дослідження симетричних та асиметричних криптографічних алгоритмів та принципів криптоаналізу	2
7	Дослідження способів використання цифрових підписів та механізмів і протоколів керування ключами.	2
8	Дослідження методів та засобів забезпечення захисту інформації та безпечного проектування програмного забезпечення	2
Разом		**15**

5. **Теми самостійної роботи**

№ з/п	Назва теми	Кількість годин
1	Основні положення теорії захисту інформації та кібербезпека.	8
2	Технології та основні шляхи забезпечення захисту інформації.	8
3	Канали витоку інформації.	8
4	Захист інформації від соціотехнічних атак.	8
5	Процеси та потоки в операційних сисетема	8
6	Захист інформації на персональних комп’ютерах.	8
7	Засоби мережевого захисту інформації.	8
8	Моделі захисту	8
9	Симетричні криптографічних алгоритми	8
10	Асиметричні криптографічні алгоритми	8
11	Принципи криптоаналізу	8
12	Цифрові підписи та механізми і протоколи керування ключами	8
13	Паролі і механізми контролю за доступом. Протоколи автентифікації	8
14	Міжмережеві екрани	8
15	Методи та засоби забезпечення захисту інформації та безпечного проектування програмного забезпечення	8
Разом		**120**

6. **Методи та засоби діагностики результатів навчання:**

- модульні тести;
- захист лабораторних робіт;
- екзамен

7. **Методи навчання*:***

- лекція (проблемна, інтерактивна);
- лабораторна робота;
- проблемне навчання;
- проєктне навчання (індивідуальне).

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. Архітектура і компоненти операційних систем		
Лабораторна робота 1.	Навчитися користуватися сервісними функціями операційних систем та вміти здійснювати базові настроювання клієнтських та серверних операційних систем, вміти аналізувати запущені процеси в операційних системах, порівнювати та оцінювати різні методи, що лежать в основі планування і диспетчеризації процесів.	**15**
Лабораторна робота 2.		**15**
Лабораторна робота 3.		**15**
Лабораторна робота 4.		**15**
Модульна контрольна робота 1.		**40**
Всього за модулем 1		**100**
Модуль 2. Файлові системи, мережеві і розподілені операційні системи, безпека операційних систем.		
Лабораторна робота 5.	Навчитися вибирати оптимальні алгоритми керування ресурсами та вирішувати задачі управління доступом до інформаційних ресурсів та процесів, вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до ресурсів і процесів операційних систем.	**15**
Лабораторна робота 6.		**15**
Лабораторна робота 7.		**15**
Лабораторна робота 8.		**15**
Модульна контрольна робота 2.		**40**
Всього за модулем 2		**100**
Навчальна частина (модулі 1 і 2)		**70**
Екзамен		**30**
Всього за курс		**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	*Терміни виконання робіт 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).*
Політика щодо академічної доброчесності	*Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Курсові роботи, 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 навчальної дисципліни (на навчальному порталі НУБіП України eLearn - https://elearn.nubip.edu.ua/course/view.php?id=28).

10. Рекомендовані джерела інформації

Основна:

1. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1,11 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.
2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
3. Гнатюк, С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк// Безпека інформації.— 2013.— Т. 19, № 2.— С. 118–129.
4. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Коропь. - Х.: Вид. ХНЕУ, 2013. - 476 с.
5. Корченко, О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О. Г. Корченко, В. Л. Бурячок, С. О. Гнатюк // Безпека інформації.— 2013.— Т. 19, № 1.— С. 40–45.
6. Мельник, С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров, О. С. Лєнков // Зб. наук. праць Військового ін-ту КНУ ім. Тараса Шевченка.— К.: ВІКНУ, 2011.— Вип. 30.— С. 159–165.
7. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша — К.: ВБ «Аванпост-Прим», 2012.— 214 с.
8. Бучик С. С. Захист інформації в інформаційно-телекомунікаційних системах : конспект лекцій / С. С. Бучик, Р. В. Нетребко. – Житомир : ЖВІ, 2018. – 196 с.
9. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: монографія/ В. Л. Бурячок.— К.: НАУ, 2013.— 432 с.

Додаткова:

10. Навчальний контент на платформі RangeForce (https://www.rangeforce.com/) за темою: Reverse Engineering (x86 Architecture; Life of Binaries; Intermediate Languages; Static Analysis; Dynamic Analysis; Capstone) наданий за проектом USAID «Cybersecurity for Critical Infrastructure in Ukraine», 2023.
11. Бучик С. С. Програмування. Основи програмування в середовищі Microsoft Visual C++ : конспект лекцій / С. С. Бучик, Р. В. Нетребко. - Житомир : ЖВІ, 2016. – 204 с.
12. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.
13. Overview of Windows Programming in C++ [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/en-us/cpp/windows/overview-of-windows-programming-in-cpp?view=msvc-150
14. Jon Erickson. Hacking: The art of exploitation. San Francisco, No Starch Press (2008), 488p.
15. Положення про порядок оцінювання знань здобувачів при кредитно-модульній системі організації навчального процесу в Київському національному університеті імені Тараса Шевченка. [Електронний ресурс]. – Режим доступу: http://nmc.univ.kiev.ua/docs/POLOJENNIA-2010-1.doc
16. «Положення про організацію освітнього процесу у Київському національному університеті імені Тараса Шевченка» від 11 квітня 2022 року. [Електронний ресурс]. – Режим доступу: http://fit.univ.kiev.ua/wp-content/uploads/2020/02/Polozhennia-pro-organizatsiyu-osvitniogo-procesu-11_04_2022.pdf
17. Про основи національної безпеки України: за станом на 20.07.2010 р. / Закон, затверджений ВР України 19 червня 2003 р., № 964-IV [Електронний ресурс].— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Урядовий кур'єр від 30.07.2003, № 139.
18. Про державну службу спеціального зв'язку та захисту інформації: за станом на 07.08.2011 р. / Закон, затверджений ВР України 23 лютого 2006 року, № 3475-IV [Електронний ресурс].— Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Урядовий кур'єр від 11.04.2006, № 68.