НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних наук

ЗАТВЕРДЖЕНО
Факультет інформаційних технологій

"____"_____20__ р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека програм та даних

Галузь знань F "Інформаційні технології"
Спеціальність F2 "Інженерія програмного забезпечення"
Освітня програма Інженерія програмного забезпечення
Факультет інформаційних технологій
Розробники: **Віктор СЕМКО, професор, к.т.н., доцент**

Київ – 2026 р.

Опис навчальної дисципліни

Дисципліна «Безпека програм та даних» спрямована на формування у студентів теоретичних знань і практичних навичок із забезпечення інформаційної безпеки в програмних, інформаційних та інформаційно-комунікаційних системах. Основна увага приділяється правовим основам захисту інформації, моделюванню загроз і порушників, принципам побудови політики безпеки, криптографічним алгоритмам та механізмам забезпечення цілісності й доступності даних. Під час навчання здобувачі опановують сучасні підходи до створення комплексних систем захисту, вивчають методи аналізу вразливостей і протидії несанкціонованому доступу. Курс забезпечує розвиток критичного мислення, здатності до проєктування захищених архітектур, розуміння технічних стандартів і регламентів. Завдяки практико-орієнтованим лабораторіям студенти набувають компетентностей у реалізації й аналізі систем криптографічного захисту та безпеки даних в ІКС.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*бакалавр*	
Спеціальність	*F2 "Інженерія програмного забезпечення"*	
Освітня програма	*Інженерія програмного забезпечення*	
Характеристика навчальної дисципліни		
Вид	*вибіркова*	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
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	8	
Лекційні заняття	*24 год.*	*год.*
Практичні, семінарські заняття	*год.*	*год.*
Лабораторні заняття	*24 год.*	*год.*
Самостійна робота	*102 год.*	*год.*
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	*4 год.*	

1. Мета, компетентності та програмні результати навчальної дисципліни

Метою вивчення дисципліни «Безпека програм та даних» є засвоєння студентами теоретичних основ і отримання практичних навиків щодо

- нормативно-правової документації і державних стандартів в галузі технічного і криптографічного захисту інформації;
- сутністю політики безпеки;
- способам визначення моделі загроз, моделі порушника;
- абстрактних моделей захисту інформації;
- моделей забезпечення цілісності і доступності;

= основними принципами функціонування програмних систем криптографічних перетворень інформації і крипто алгоритмами;

- принципами побудови систем захисту ресурсів інформаційно-комунікаційних систем.

Дисципліна «Безпека програм та даних» забезпечує формування таких компетентностей (у відповідності із стандартом вищої освіти за спеціальністю 122 «Комп'ютерні науки»):

- здатність застосовувати знання у практичних ситуаціях;
- здатність вчитися й оволодівати сучасними знаннями;
- здатність проектувати та розробляти засоби захисту від несанкціонованого доступу до ресурсів програмних, інформаційних та інформаційно-комунікаційних систем у відповідності з моделями, методами й алгоритмами, які реалізують політику безпеки інформації;
- здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення.

Завдання:

- засвоєння структури нормативно-правової бази, яка регламентує використання технічних засобів забезпечення автоматизованої обробки інформації;
- засвоєння принципів побудови комплексів засобів захисту (КЗЗ) НСД в програмних системах (ПС), інформаційних системах (ІС) та інформаційно-комунікаційних системах (ІКС);
- засвоєння принципів функціонування засобів захисту інформації (ЗЗІ) в ПС, ІС та ІКС;
- засвоєння порядку застосування комплексу засобів інформації (КЗЗ) при побудові комплексних систем захисту інформації (КСЗІ).

У результаті вивчення навчальної дисципліни студент повинен

знати:

- структуру нормативно-правової бази і державних стандартів, які регламентують порядок виконання робіт при створенні і впровадженні систем захисту ресурсів інформаційно-комунікаційних систем (ІКС) від несанкціонованого доступу (НСД);
- порядок розробки політики безпеки автоматизованих систем;
- принципи побудови КЗЗ інформації від НСД.
- принципи функціонування ЗЗІ та порядок їх застосування при побудові КЗЗ і КСЗІ.
- порядок створення і впровадження систем захисту ресурсів інформаційно-комунікаційних систем.;

вміти;

- обирати нормативні документи, які регламентують використання технічних засобів забезпечення автоматизованої обробки інформації;
- розробляти політику безпеки автоматизованих систем, виходячи з розуміння сутності функціональних послуг безпеки у відповідності з обраними моделями.

Програмні результати навчання (ПРН):

ПР06. Уміння вибирати та використовувати відповідну задачі методологію створення систем захисту інформації.

ПР07. Знати і застосовувати на практиці фундаментальні концепції, парадигми і

основні принципи створення і впровадження технологій захисту інформації від несанкціонованого доступу в автоматизованих системах.
ПР12. Застосовувати на практиці ефективні підходи щодо проєктування систем захисту інформації від несанкціонованого доступу.
ПР13. Знати і застосовувати методи і моделі розробки політики безпеки ресурсів ПС, ІС і ІКС.
ПР15. Мотивовано обирати способи реалізації функціональних послуг безпеки.

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. Теоретичні основи інформаційної безпеки програмних систем													
Тема 1. Основні поняття та визначення	1	16	2		2		12						
Тема 2. Основні поняття захисту інформації та моделі опису процесів функціонування автоматизованих систем.	2	16	2		2		12						
Тема 3. Визначення і абстрактні моделі управління безпекою в інформаційних системах.	3, 4	20	4		4		12						
Тема 4. Помилки, ризики і якість програмних засобів.	5, 6	22	4		4		14						
Разом за модулем 1	74		12		12		50						
Модуль 2 Криптографічні методи та технології захисту інформації													
Тема 5. Принципи функціонування програмних систем криптографічних перетворень інформації. Основні алгоритми.	7, 8, 9	34	6		6		26						
Тема 6. Захист інформації в мультимедійних інформаційно-комунікаційних системах.	10,11, 12	26	6		6		26						
Разом за модулем 2	76		12		12		52						
Усього годин													
Усього годин	**150**		**24**		**24**		**102**						

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Основні поняття та визначення.	2
2	Основні поняття захисту інформації та моделі опису процесів функціонування автоматизованих систем.	2

№ з/п	Назва теми	Кількість годин
3	Визначення і абстрактні моделі управління безпекою в інформаційних системах. Частина 1	2
4	Визначення і абстрактні моделі управління безпекою в інформаційних системах. Частина 2	2
5	Помилки, ризики і якість програмних засобів. Частина 1	2
6	Помилки, ризики і якість програмних засобів. Частина 2	2
7	Принципи функціонування програмних систем криптографічних перетворень інформації. Основні алгоритми. Частина 1	2
8	Принципи функціонування програмних систем криптографічних перетворень інформації. Основні алгоритми. Частина 2	2
9	Принципи функціонування програмних систем криптографічних перетворень інформації. Основні алгоритми. Частина 3	2
10	Захист інформації в мультимедійних ІКС. Частина 1	2
11	Захист інформації в мультимедійних ІКС. Частина 2	2
12	Захист інформації в мультимедійних ІКС. Частина 3	2
Разом		24

4. Теми лабораторних (практичних, семінарських) занять

№ з/п	Назва теми	Кількість годин
1	Дослідження програмного засобу захисту інформації “Лоза-1”.	2
2	Використання концепції ієрархічної декомпозиції при побудові систем захисту.	2
3	Дослідження функціонування злоякісного програмного коду (комп’ютерного вірусу) в обчислювальному середовищі під управлінням операційної системи Windows.	2
4	Дослідження організаційних засад забезпечення безпеки мережевої інфраструктури.	2
5	Дослідження системи аналізу захищеності мережі.	*2*
6	Дослідження технології використання антивірусу Windows Defender.	2
7	Дослідження технології захисту ресурсів при обміні електронними документами в системі державного управління.	2
8	Дослідження технології захисту інформації в автоматизованій системі медичного призначення.	4
9	Дослідження алгоритму формування загального секретного ключа учасників інформаційного обміну у відповідності зі схемою відкритого ключового обміну.	4
10	Дослідження програмного засобу захисту інформації “Лоза-1”.	2
Разом за курс		**24**

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Основні поняття та визначення.	12
2	Основні поняття захисту інформації та моделі опису процесів функціонування автоматизованих систем.	12
3	Визначення і абстрактні моделі управління безпекою в інформаційних системах.	12
4	Помилки, ризики і якість програмних засобів.	14

№ з/п	Назва теми	Кількість годин
5	Принципи функціонування програмних систем криптографічних перетворень інформації. Основні алгоритми.	26
6	Захист інформації в мультимедійних інформаційно	26
Разом за курс		**102**

6. Методи та засоби діагностики результатів навчання:

(вибрати необхідне чи доповнити)

- усне та письмове опитування;
- співбесіда;
- тестування;
- захист лабораторних робіт.

7. Методи навчання *(вибрати необхідне чи доповнити):*

- метод практико-орієнтованого навчання;
- кейс-метод;
- метод навчання через дослідження;

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. Теоретичні основи інформаційної безпеки програмних систем		
Лекція 1.	Студент повинен засвоїти базові поняття та підходи до забезпечення інформаційної безпеки, оволодіти методами ідентифікації загроз, моделювання порушників та формування політики безпеки в автоматизованих системах. Очікується, що студент зможе застосовувати абстрактні моделі управління безпекою, розуміти принципи оцінки надійності та якості програмних засобів, а також аналізувати ризики, пов'язані з уразливостями систем. Практичні завдання спрямовані на формування компетентностей щодо виявлення і аналізу потенційних загроз у середовищах обробки даних, а також вивчення організаційних і технічних підходів до захисту інформації. Підготувати та захистити звіти з лабораторних робіт.	1
Лабораторна робота 1.		5
Самостійна робота 1.		2
Лекція 2.		1
Лабораторна робота 1.		5
Самостійна робота 1.		2
Лекція 3.		1
Лабораторна/практична робота 2.		5
Самостійна робота 2.		2
Лекція 4.		1
Лабораторна робота 2.		5
Самостійна робота 2.		2
Лекція 5.		1
Лабораторна робота 3.		5
Самостійна робота 3.		3
Лекція 6.		1
Лабораторна робота 3.		5
Самостійна робота 3.		3
Лекція 7.		1
Лабораторна 4.		5
Самостійна робота 4.		4
Лекція 8.		1
Лабораторна робота 4.		5
Самостійна робота 4.		4

Вид навчальної діяльності	Результати навчання	Оцінювання
Модульна контрольна робота 1.		30
Всього за модулем 1		**100**
Модуль 2. Криптографічні методи та технології захисту інформації		
Лекція 9.	Студент повинен оволодіти принципами функціонування програмних систем криптографічних перетворень інформації, вивчити базові та сучасні алгоритми шифрування, а також засоби захисту даних у мультимедійних інформаційно-комунікаційних системах. Студент має засвоїти методи реалізації криптографічного захисту, зокрема при формуванні, обміні та зберіганні конфіденційної інформації, а також здобути практичні навички застосування програмних засобів для забезпечення цілісності, автентичності та конфіденційності даних. Результатом навчання є здатність аналізувати загрози для медичних, державних та корпоративних ІКС, інтегрувати засоби криптозахисту в архітектуру систем і здійснювати оцінювання їх ефективності. Підготувати та захистити звіти з лабораторних робіт.	1
Лабораторна робота 5.		6
Самостійна робота 5.		2
Лекція 10.		1
Лабораторна робота 5.		6
Самостійна робота 5.		2
Лекція 11.		1
Лабораторна/практична робота 6.		6
Самостійна робота 6.		2
Лекція 12.		1
Лабораторна робота 7.		6
Самостійна робота 7.		3
Лекція 13.		1
Лабораторна робота 8.		6
Самостійна робота 8.		4
Лекція 12.		1
Лабораторна робота 7.		6
Самостійна робота 7.		4
Лабораторна робота 8.		6
Самостійна робота 8.		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 (*за наявності*)		**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	*НАПРИКЛАД:* 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	*НАПРИКЛАД:* 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	*НАПРИКЛАД:* відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в онлайн 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=3896);
- посилання на цифрові освітні ресурси;
- підручники, навчальні посібники, практикуми;
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти денної та заочної форм здобуття вищої освіти;
- програма навчальної (виробничої) практики навчальної дисципліни (якщо вона передбачена навчальним планом).

10. Рекомендовані джерела інформації

10.1 Основні джерела

1. Богуш В.М., Давидьков О.А. Теоретичні основи захищених інформаційних технологій. – К.: ДУІКТ, 2010. – 414 с.
2. Тарнавський Ю.А. Технології захисту інформації. – К.: КПІ, 2018. – 161 с.
3. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів,БаК, 2003. – 144 с.
4. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – Киев,Корнийчук, 2000. – 152 с.
5. Басюк Т.М., Жежнич П.І. Методи та засоби мультимедійних інформаційних систем. – Львів: Вид-во Львівської політехніки, 2015. – 428 с. – 331.
6. Стеклов В. К., Беркман Л.Н. Проектування телекомунікаційних мереж Київ : Техніка, 2002. 792 с.
7. Семко В.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В.Л.Бурячок, В.В.Семко, П.М.Складанний, Н.В. Лукова-Чуйко – К.: ДУТ - КНУ, 2016. – 178с.
8. Семко В.В. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

10.2 Додаткові рекомендовані джерела

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. 608 с.

2. Юдін О.К., Корченко О.Г., Конахович В.Г. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ НВП "ІНТЕРСЕРВІС", 2009. 716 с.

3. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний *захист інформації. Основні положення від 01.07.1997.*

4. Державний стандарт України ДСТУ 3396.1 -96. Захист інформації. Технічний захист інформації. Порядок проведення робіт від 01.07.1997.

5. Державний стандарт України ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. від 01.07.1997.

6. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99р. № 22.

7. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.

8. НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

9. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

10. НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

11. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі від 08.11.2005 р. №125.

12. НД ТЗІ 2.2-005-08 Технічний захист інформації. Захист інформації, яку обробляють засобами електронної обчислювальної техніки на об'єктах інформаційної діяльності, від витоку інформації за рахунок побічних електромагнітних випромінювань і наводів. Норми ефективності захисту.

13. НД ТЗІ 2.2-006-08 Захист інформації на об'єкті інформаційної діяльності. Норми протидії технічній розвідці в акустичному і віброакустичному каналах витоку інформації.