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

ЗАТВЕРДЖЕНО
Факультет інформаційних технологій
Протокол №12 від «11» червня» 2026р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в комп'ютерних системах

Галузь знань F – Інформаційні технології
Спеціальність F7 - Комп'ютерна інженерія
Освітня програма Комп'ютерна інженерія
Факультет (ННІ) – Інформаційних технологій
Розробники: к.т.н., доцент Андрій САГУН
(посада, науковий ступінь, вчене звання)

Київ – 2026 р.

Опис навчальної дисципліни

Дисципліна вивчає теоретичну та практичну підготовка здобувачів до розробки та застосування сучасних програмно-апаратних систем захисту інформації в різних установах та на підприємствах, зокрема АПК.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*бакалавр*	
Спеціальність	*123 - Комп'ютерна інженерія*	
Освітня програма	*Комп'ютерна інженерія*	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	3	
Курсовий проект (робота) (за наявності)	-	
Форма контролю	*іспит*	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	2	-
Семестр	4	-
Лекційні заняття	*48 год.*	*год.*
Практичні, семінарські заняття	- *год.*	*год.*
Лабораторні заняття	*48 год.*	*год.*
Самостійна робота	*54 год.*	*год.*
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	*8 год.*	

1. Мета, компетентності та програмні результати навчальної дисципліни

Мета вивчення дисципліни «Захист інформації в комп'ютерних системах» є формування теоретичних знань і практичних навичок, необхідних для забезпечення інформаційної безпеки, а саме збереження конфіденційності**,** цілісності та доступності даних.

Перелік освітніх компонент, які передують вивченню навчальної дисципліни *(за їх наявності)**:*** Комп'ютерні системи, Системне програмування.

Набуття компетентностей:

Інтегральна компетентність (ІК):

Загальні компетентності (ЗК):

1. Базові знання технічних характеристик, конструктивних особливостей, застосування правил експлуатації комп'ютерних систем, мереж та програмно-технічних засобів.

2. Здатність використовувати методи фундаментальних і прикладних дисциплін для опрацювання, аналізу і синтезу результатів професійних досліджень.

3. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем та мереж, Інтернет додатків, кібер-фізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.

6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних

систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

Спеціальні (фахові) компетентності (СК):

3. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем та мереж, Інтернет додатків, кібер-фізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування

5. Здатність створювати системне та прикладне програмне забезпечення комп'ютерних систем та мереж.

11. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.

Програмні результати навчання (ПРН):

1. Знати і розуміти наукові і математичні положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

2. Знати основи професійно-орієнтованих дисциплін спеціальності.

4. Мати знання з новітніх технологій в галузі комп'ютерної інженерії.

5. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи відомі методи.

7. Вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для спеціальності.

8. Вміти системно мислити та застосовувати творчі здібності до формування принципово нових ідей.

9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.

16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

21. Відповідально ставитись до виконуваної роботи та досягати поставленої мети з дотриманням вимог професійної етики.

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.
Змістовий модуль 1. Правила проектування послуг безпеки та платформ забезпечення механізмів захисту інформації													
Тема 1. Базові поняття про захист інформаціїі в ІКС. Проектування послуг безпеки		8	4		-		4						
Тема 2. Хмарні платформи та системи підтримки і адміністрування хмарних платформ. Забезпечення		10	4		4		2						

систем розгортання та адміністрування послуг безпеки комп'ютерних корпоративних мереж													
Тема 3. Політики безпеки та ризики порушення політик інформаційної безпеки в КС. Розгортання віртуальної ІКС		16	4		8		4						
Тема 4. Створення хмарної платформи під заплановані заходи що до впровадження механізмів реалізації послуг безпеки		8	2		2		4						
Разом за змістовим модулем 1		**42**	**14**		**14**		**16**						
Змістовий модуль 2.													
Тема 5. Вибір та налаштування компонентів ПЗ WS 2012 з врахуванням моделі безпеки ІКС для підприємства		14	4		4		6						
Тема 6. Планування доменної структури корпоративної мережі, як основи вузлів безпеки для об'єктів та суб'єктів доступу до інформації корпоративної мережі		12	4		4		4						
Тема 7. Об'єкти та суб'єкти доступу та механізми доступу в рамах корпоративної мережі. Групи доступу та безпеки в ІКС		14	4		4		6						
Тема 8. Групові політики для суб'єктів та груп безпеки і розповсюдження у WS. Правила проектування та вибору зон дії групових політик у WS 2012		16	6		6		4						
Разом за змістовим модулем 2		**56**	**18**		**18**		**20**						
Змістовий модуль 3.													
Тема 9. Проектування послуг забезпечення доступності та цілісності даних в корпоративних мережах. Технологія RAID та її реалізація у		14	4		4		6						

WS 2012													
Тема 10. Механізми забезпечення доступності даних в КС. Реплікація даних DC. Створення механізму реплікації даних.		18	6		6		6						
Тема 11. Корпоративні електронні поштові сервіси та їх проектування та налаштування у WS.		18	6		4		8						
Разом за змістовим модулем 3		**50**	**16**		14		20						
Всього годин за курс		**150**	**48**	**-**	**48**		**54**						

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Базові поняття про захист інформаціїї в ІКС. Проектування послуг безпеки	4
2	Хмарні платформи та системи підтримки і адміністрування хмарних платформ. Забезпечення систем розгортання та адміністрування послуг безпеки комп'ютерних корпоративних мереж	4
3	Політики безпеки та ризики порушення політик інформаційної безпеки в КС. Розгортання віртуальної ІКС, вибір та налаштування маршрутизуючих пристроїв	4
4	Створення хмарної платформи під заплановані заходи що до впровадження механізмів реалізації послуг безпеки	2
5	Вибір та налаштування компонентів ПЗ WS 2012 з врахуванням моделі безпеки ІКС для підприємства	4
6	Планування доменної структури корпоративної мережі, як основи вузлів безпеки для об'єктів та суб'єктів доступу до інформації корпоративної мережі	4
7	Об'єкти та суб'єкти доступу та механізми доступу в рамах корпоративної мережі. Групи доступу та безпеки в ІКС	4
8	Групові політики для суб'єктів та груп безпеки і розповсюдження у WS. Правила проектування та вибору зон дії групових політик у WS 2012	6
9	Проектування послуг забезпечення доступності та цілісності даних в корпоративних мережах. Технологія RAID та її реалізація у WS 2012	4
10	Механізми забезпечення доступності даних в КС. Реплікація даних DC. Створення механізму реплікації даних.	6
11	Корпоративні електронні поштові сервіси та їх проектування та налаштування у WS.	4

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз ризиків порушення політики інформаційної безпеки об'єкта інформатизації та планування заходів що до впровадження механізмів реалізації послуг безпеки	2
2	Створення хмарної платформи під заплановані заходи що до	4

	впровадження механізмів реалізації послуг безпеки. Конфігурування елементів комп'ютерної мережі	
3	Налаштування та розгортання послуг безпеки Windows Server в хмарному середовищі	8
4	Встановлення та налаштування ролей сервера та компонентів Active Directory WS 2012 r2. Створення каталогу AD, доменної структури підприємства в середовищі Windows Server 2012 r2	2
5	Побудова концептуальної моделі корпоративної безпеки у WS 2012 та розгортання основних одиниць безпеки ІКС – доменів лісу	6
6	Проектування та реалізація моделі розмежування прав доступу до інформаційних ресурсів корпоративної мережі	4
7	Забезпечення послуг доступності та цілісності даних. Механізми автовідновлення даних в технології реплікації Windows Server	6
8	Забезпечення доступності, цілісності та відмовостійкості даних, в рамках технології RAID	6
9	Проектування та реалізація групових політик для учасників корпоративної мережі Windows Server	6
10	Встановлення та налаштування захищеного сервісу корпоративної електронної пошти на базі серверу MS Exchange. Адміністрування корпоративних поштових облікових записів	4

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Етапи планування систем та сервісів корпоративних мереж	2
2	Хмарні системи та моделі хмарних сервісів типу PaaS, SaaS, IaaS	2
3	Створення політик безпеки та їх інтерпретація при проектування сервісів та послуг безпеки в ІКС	4
4	Вибір та налаштування серверних ролей та компонентів під корпоративні задачі захисту інформації в ІКС підприємства	4
5	Моделі безпеки, їх види та типи.	6
6	Домен, як одиниця безпеки. Довірчі зв'язки та їх організації з врахуванням потреб корпоративної політики безпеки	4
7	Моделі розмежування прав доступу. Авторизація та захист з'єднання між логічними одиницями КМ, налаштування Kerberos	6
8	Технології захисту даних та їх проектування в корпоративних мережах.	4
9	Реплікація та резервування при захисті корпоративної інформації. Опції налаштування та застосування технологій реплікації у WS 2012	6
10	Принципи та алгоритмі проектування групових політик. Інструментальні засоби застосування групових політик в КМ на базі WS 2012	6
11	Корпоративні поштові сервіси та принципи їх налаштування і маршрутизації. Налаштування фільтрів та систем безпеки корпоративної пошти	8
	Разом	**150**

6. Теми семінарських занять (не передбачені навчальним планом)

7. Теми практичних занять (не передбачені навчальним планом)

8. Методи та засоби діагностики результатів навчання:
(вибрати необхідне чи доповнити)

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

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

- метод проблемного навчання;
- метод практико-орієнтованого навчання;
- метод командної роботи, мозкового штурму
- метод гейміфікованого навчання.

10. 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».

10.1 Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Змістовий модуль 1.		
Лабораторна робота 1 - Аналіз ризиків порушення політики інформаційної безпеки об'єкта інформатизації та планування заходів що до впровадження механізмів реалізації послуг безпеки	5. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті. 6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи відомі методи.	4
Лабораторна робота 2 - Створення хмарної платформи під заплановані заходи що до впровадження механізмів реалізації послуг безпеки. Створення вузлів мережевої безпеки	1. Знати і розуміти наукові і математичні положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж. 4. Мати знання з новітніх технологій в галузі комп'ютерної інженерії. . Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.	5
Лабораторна робота 3 - Налаштування та розгортання послуг безпеки Windows Server в хмарному середовищі	2. Знати основи професійно-орієнтованих дисциплін спеціальності. 7. Вміти застосовувати знання для розв'язування задач аналізу та синтезу	5

	засобів, характерних для спеціальності.	
Самостійна робота 1 - Етапи планування систем та сервісів корпоративних мереж	1. Знати і розуміти наукові і математичні положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж. 4. Мати знання з новітніх технологій в галузі комп'ютерної інженерії.	2
Самостійна робота 2 - Хмарні системи та моделі хмарних сервісів типу PaaS, SaaS, IaaS		2
Самостійна робота 3 - Створення політик безпеки та їх інтерпретація при проектування сервісів та послуг безпеки в ІКС		2
Самостійна робота 4 - Вибір та налаштування серверних ролей та компонентів під корпоративні задачі захисту інформації в ІКС підприємства		2
Всього за модулем 1		**22**
Змістовий модуль 2.		
Лабораторна робота 4 - Встановлення та налаштування ролей сервера та компонентів Active Directory WS 2012 r2. Створення каталогу AD, доменної структури підприємства в середовищі Windows Server 2012 r2	16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення. 19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.	4
Лабораторна робота 5 - Побудова концептуальної моделі корпоративної безпеки у WS 2012 та розгортання основних одиниць безпеки ІКС – доменів лісу	9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.	5
Лабораторна робота 6 - Проектування та реалізація моделі розмежування прав доступу до інформаційних ресурсів корпоративної мережі	14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.	4
Самостійна робота 5 - Моделі безпеки, їх види та типи.	8. Вміти системно мислити та застосовувати творчі здібності до формування принципово нових ідей. 9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності	2
Самостійна робота 6 - Домен, як одиниця безпеки. Довірчі зв'язки та їх організації з врахуванням потреб корпоративної політики безпеки		2
Самостійна робота 7 - Моделі розмежування прав доступу. Авторизація та захист з'єднання між логічними одиницями КМ, налаштування Kerberos		2
Самостійна робота 8 - Технології захисту даних та їх проектування в корпоративних мережах		2
Всього за модулем 2		**21**
Змістовний модуль 3.		
Лабораторна робота 7 - Забезпечення	7. Вміти застосовувати знання для	6

послуг доступності та цілісності даних. Механізми автовідновлення даних в технології реплікації Windows Server	розв'язування задач аналізу та синтезу засобів, характерних для спеціальності.	
Лабораторна робота 8 - Забезпечення доступності, цілісності та відмовостійкості даних, в рамках технології RAID	10. Вміти розробляти системне і прикладне програмне забезпечення для вбудованих і розподілених застосувань, мобільних систем, розраховувати, експлуатувати, типове для спеціальності обладнання	5
Лабораторна робота 9 - Проектування та реалізація групових політик для учасників корпоративної мережі Windows Server	13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.	6
Лабораторна робота 10 - Встановлення та налаштування захищеного сервісу корпоративної електронної пошти на базі серверу MS Exchange. Адміністрування корпоративних поштових облікових записів	21. Відповідально ставитись до виконуваної роботи та досягати поставленої мети з дотриманням вимог професійної етики.	5
Самостійна робота 9 - Реплікація та резервування при захисті корпоративної інформації. Опції налаштування та застосування технологій реплікації у WS 2012	9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності 10. Вміти розробляти системне і прикладне програмне забезпечення для вбудованих і розподілених застосувань, мобільних систем, розраховувати, експлуатувати, типове для спеціальності обладнання	2
Самостійна робота 10 - Принципи та алгоритмі проектування групових політик. Інструментальні засоби застосування групових політик в КМ на базі WS 2012		2
Самостійна робота 11 - Корпоративні поштові сервіси та принципи їх налаштування і маршрутизації. Налаштування фільтрів та систем безпеки корпоративної пошти		2
Всього за модулем 3		**28**
		(М1 + М2)*0,7 ≤ 70
Залік		**30**
Всього за курс		**(Навчальна робота + екзамен) ≤ 100**

8.1. 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

8.2. Політика оцінювання

Політика щодо	Роботи, які здаються із порушенням термінів без поважних причин,

дедлайнів та перескладання	оцінюються на нижчу оцінку (пропорційно інтервалів пропущеної дати складання). Перескладання модульних контрольних та тестів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).
Політика щодо академічної доброчесності	Списування під час заліку заборонено (в т.ч. із використанням мобільних девайсів). Практичні роботи мають бути виконані виключна за індивідуальними завданнями варіантів.
Політика щодо відвідування	Відвідування занять є обов'язковим. За об'єктивних причин (хвороба, участь в заходах від кафедри або факультету, міжнародне стажування). В узгоджених офіційно випадках навчання може відбуватись індивідуально (в он-лайн формі)

11. Навчально-методичне забезпечення:

Електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - https://elearn.nubip.edu.ua/course/view.php?id=2773), що складається з:

- лекцій та їх презентації (в електронному вигляді);
- завдань для виконання практичних робіт;
- блоку підсумкового оцінювання знань.
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти всіх форм навчання вищої освіти;
- програма навчальної дисципліни.

12. Рекомендовані джерела інформації

1. Операційні системи та комп'ютерні мережі [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Автоматизація та комп'ютерно-інтегровані технології кібер-енергетичних систем» спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології», освітньо-професійною програмою / КПІ ім. Ігоря Сікорського ; уклад. А. В. Сагун, В. Б. Бобков. – Електронні текстові данні (1 файл 10 Мбайт). – Київ : КПІ ім. Ігоря Сікорського», 2022. – 164 с. – Назва з екрана.
2. НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
3. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)
4. НД ТЗІ 2.5-004-99. Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. — Чинний від 2000-01-01. — К.: Держтехзахист інформації, 1999. — 24 с
5. НД ТЗІ 2.5-005-99. Порядок проведення атестації комплексної системи захисту інформації в автоматизованій системі [Електронний ресурс]. — К.: Держтехзахист інформації, 1999. — 36 с. — Режим доступу: *URL https://tzi.com.ua/downloads/2.5-005%20-99.pdf*