НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра автоматики та робототехнічних систем ім. акад. І.І. Мартиненка

ЗАТВЕРДЖУЮ
Директор ННІ енергетики,
автоматики і енергозбереження
_____ Віктор КАПЛУН
"____"_____20____ р.

СХВАЛЕНО
на засіданні кафедри АРС
протокол № 11 від 29.05.2026 р.
Завідувач кафедри
_____Олексій ОПРИШКО

РОЗГЛЯНУТО
Гарант ОНП Автоматизація,
комп'ютерно-інтегровані технології
та робототехніка
_____В'ячеслав ІВАЩУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Захист інформації в системах автоматизації»

Галузь знань G – Інженерія, виробництво та будівництво
Спеціальність G7 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка
Освітня програма «Автоматизація та комп'ютерно-інтегровані технології та робототехніка»
ННІ Енергетики, автоматики і енергозбереження

Розробник: Валерій КОВАЛЬ, проф. каф.

Київ – 2026 р.

Опис навчальної дисципліни. В дисципліні "Захист інформації в системах автоматизації" розглядаються основні поняття захисту інформації в системах автоматизації, принципи побудови комплексних систем захисту інформації, зазначаються типові вразливості систем, проводиться аналіз систем на предмет захищеності та визначаються нормативні документи в галузі захисту інформації в системах автоматизації. Визначаються правові, організаційні та технічні методи захисту інформації. Отримуються практичні навички застосування сучасних технологій забезпечення інформаційної безпеки в системах автоматизації.

Завданнями дисципліни є:

- ознайомлення з базовими поняттями, технологією та визначеннями теорії захисту інформації;
- вивчення основних формальних та неформальних підходів до розгляду питань теорії захисту інформації;
- вивчення нормативних документів в галузі захисту інформації в системах автоматизації;
- отримання практичних навичок застосування сучасних технологій забезпечення інформаційної безпеки в системах автоматизації.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*Магістр*	
Спеціальність	G7 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»	
Освітня програма	Автоматизація,комп'ютерно-інтегровані технології та робототехніка	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5,0	
Кількість змістових модулів	2	
Курсовий проект (робота) (за наявності)	-	
Форма контролю	*екзамен*	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Денна форма здобуття вищої освіти	Заочна форма здобуття вищої освіти
Курс (рік підготовки)	2	
Семестр	2	
Лекційні заняття	10 год.	
Практичні, семінарські заняття	нема	
Лабораторні заняття	30 год.	
Самостійна робота	110 год.	
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	4 год.	

1. **Мета, компетентності та програмні результати навчальної дисципліни**

Мета – формування у студентів знань про методи і способи захисту інформації та отримання практичних навичок застосування сучасних технологій забезпечення інформаційної безпеки в системах автоматизації.

Набуття компетентностей:

інтегральна компетентність (ІК): Здатність розв'язувати складні задачі і проблеми у галузі автоматизації, комп'ютерно-інтегровних технологій та робототехніки або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і суперечливістю вимог.

загальні компетентності (ЗК):_____

спеціальні (фахові) компетентності (СК): СК2. Здатність проектувати та впроваджувати високонадійні системи автоматизації та їх прикладне програмне забезпечення, для реалізації функцій управління та опрацювання інформації, здійснювати захист прав інтелектуальної власності на нові проектні та інженерні рішення;

СК7. Здатність застосовувати спеціалізоване програмне забезпечення та цифрові технології для розв'язання складних задач і проблем автоматизації та комп'ютерно-інтегрованих технологій.

Програмні результати навчання (ПРН): ПРН2. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів;

ПРН3. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки, а також критичне осмислення сучасних проблем у сфері автоматизації та комп'ютерно-інтегрованих технологій для розв'язування складних задач професійної діяльності;

ПРН9. Розробляти функціональну, організаційну, технічну та інформаційну структури систем автоматизації складними технологічними та організаційнотехнічними об'єктами, розробляти програмно-технічні керуючі комплекси із застосовуванням мережевих та інформаційних технологій, промислових контролерів, мехатронних компонентів, робототехнічних пристроїв, засобів людино-машинного інтерфейсу та з урахуванням технологічних умов та вимог до управління виробництвом.

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.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Модуль 1. ***Концептуальні засади захисту інформації в автоматизованих системах.***													
Тема 1. Предмет та об'єкт захисту у інформаційній безпеці. Комп'ютерні системи і мережі.		11	2		2		7						
Тема 2. Завадозахищеність сигналів в комп'ютерних мерехах за різних методів модуляції кіберінформації		9	-		2		7						
Тема 3. Проблеми		9	-		2		7						

захищеності цифрових сигналів керування в системах автоматизації Взаємодія відкритих систем. Інформаційна безпека протоколів. IP-протокол та атаки, пов'язані з адресацією.													
Тема 4. Завадозахищеність цифрових сигналів керування систем автоматизації за різних умов їх оброблення.		9	-		2		7						
Тема 5. Загрози безпеці інформації. Поняття та класифікація загроз інформації в автоматизованих системах. Характеристика загроз безпеки інформації. Несанкціонований доступ.		11	2		2		7						
Тема 6. Моделі та аналіз каналів витоку кіберінформації в системах автоматизації.		9	-		2		7						
Тема 7. Технічні канали витоку інформації. Поняття порушника інформаційної безпеки. Модель порушника.		12	2		2		8						
Разом за модулем 1		70	6		14		50						
Модуль 2. ***Комплексний захист інформації автоматизованих систем.***													
Тема 8. Концепція захисту інформації. Шляхи забезпечення безпеки інформації. Політика безпеки інформації.		9	-		2		7						
Тема 9. Забезпечення комплексності вирішення завдань інформаційної безпеки. Діяльність міжнародних організацій, що діють у сфері інформаційної безпеки.		11	2		2		7						
Тема 10. Стандарти IEC/ISA 62443 для		9	-		2		7						

підтримки безпечної експлуатації промислових систем автоматизації.													
Тема 11. Міжнародні стандарти проєктування та експлуатації систем автоматизації. Стандартизація в сфері менеджменту інформаційної безпеки.		9	-		2		7						
Тема 12. Аналіз застосування термінів, визначених нормативними документами інформаційної безпеки, для підготовки документів щодо створення комплексної системи захисту інформації.		10	-		2		8						
Тема 13. Концепція, стратегія та архітектура захисту інформації. Етапи розробки. Політика захисту інформації. Положення про службу захисту інформації.		12	2		2		8						
Тема 14. Управління ризиками. Загрози, прогнозування та оцінка їх наслідків. Ризик-менеджмент.		10	-		2		8						
Тема 15. Етапи створення комплексної системи захисту інформації (КСЗІ). Державна експертиза КСЗІ та супровід в період функціонування.		10	-		2		8						
Разом за модулем 2		80	4		16		60						
Усього годин	150		10		30		110						
Курсовий проект (робота) з_____ (якщо є в навчальному плані)			-	-	-		-						
Усього годин	150		10		30		110						

3.Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Предмет та об'єкт захисту у інформаційній безпеці. Комп'ютерні системи і мережі.	2
5	Загрози безпеці інформації. Поняття та класифікація загроз інформації в автоматизованих системах. Характеристика загроз безпеки інформації. Несанкціонований доступ..	2
7	Технічні канали витоку інформації. Поняття порушника інформаційної безпеки. Модель порушника.	2
9	Забезпечення комплексності вирішення завдань інформаційної безпеки. Діяльність міжнародних організацій, що діють у сфері інформаційної безпеки.	2
13	Концепція, стратегія та архітектура захисту інформації. Етапи розробки. Політика захисту інформації. Положення про службу захисту інформації.	2

4.Теми лабораторних (практичних, семінарських) занять

№ з/п	Назва теми	Кількість годин
1	Дослідження завадозахищеності сигналів в системах автоматизації за різних методів модуляції кіберінформації.	4
2	Дослідження завадозахищеності цифрових сигналів керування систем автоматизації від впливу завад за різних умов оброблення.	4
3	Дослідження процесів кодування кіберінформації в системах автоматизації	4
4	Дослідження генератора псевдовипадкової послідовності, скремблера та дескремблера кіберінформації систем автоматизації.	4
5	Аналіз стандартів IEC/ISA 62443 для підтримки безпечної експлуатації промислових систем автоматизації.	4
6	Аналіз застосування термінів, визначених нормативними документами інформаційної безпеки, для підготовки документів щодо створення комплексної системи захисту інформації.	4
7	Аналіз обєктів автоматизації та підготовка загальних положень, розділів 1 і 2 «Положення про службу захисту інформації».	2
8	Моделювання та дослідження технічних засобів захисту інформації в системах автоматизації на основі програмованих логічних інтегральних схем.	4

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1.	Вкажіть у чому складність створення систем захисту інформації.	3
2.	Опишіть поняття захисту інформації в ІТС та її роботи з організації.	3
3.	Опишіть поняття теорії захисту інформації та її періоди розвитку.	3
4.	Наведіть особливості теорії захисту інформації.	4
5.	Вкажіть у чому полягають формальні та неформальні підходи до	3

	розгляду питань теорії захисту інформації.	
6.	Вкажіть, які є напрямки розвитку теорії захисту інформації.	3
7.	Вкажіть, що собою представляє загроза безпеки КС.	3
8.	Вкажіть, які загрози безпеки КС відносять до випадкових.	4
9.	Вкажіть, які загрози безпеки КС відносять до навмисних.	3
10.	Вкажіть, що собою представляє загроза розкриття і їх протидія.	3
11.	Вкажіть, що собою представляє загроза порушення цілісності і їх протидія.	3
12.	Вкажіть, що собою представляє загроза відмови в обслуговуванні.	3
13.	Вкажіть напрями повсякденної діяльності в ІТС для підтримки її працездатності.	3
14.	Вкажіть якими послугами забезпечується доступність в ІТС.	3
15.	Вкажіть, що собою представляє спосіб несанкціонованого доступу та які мети переслідує зловмисник.	3
16.	Вкажіть, що таке комп'ютерне піратство та категорії порушників безпеки.	3
17.	Вкажіть, що визначає модель порушника безпеки.	3
18.	Опишіть концепцію захисту інформації.	4
19.	Опишіть стратегію захисту інформації та ієрархічний підхід до забезпечення безпеки інформації.	3
20.	Опишіть етапи розробки концепції захисту інформації.	3
21.	Вкажіть поняття політики захисту інформації.	3
22.	Охарактеризуйте правові та організаційно-адміністративні заходи протидії комп'ютерним злочинам.	3
23.	Охарактеризуйте інженерно-технічні заходи протидії комп'ютерним злочинам.	4
24.	Вкажіть комплекс задач при розробці політики безпеки.	3
25.	Вкажіть правила забезпечення політики безпеки інформації.	3
26.	Опишіть перший етап проектування та реалізації системи захисту.	3
27.	Вкажіть, які ймовірні загрози виділяють у комп'ютерних мережах.	3
28.	Вкажіть, яким заходам повинна визначатися політика безпеки.	3
29.	Опишіть другий етап проектування та реалізації системи захисту – реалізація політики безпеки.	3
30.	Опишіть третій етап проектування та реалізації системи захисту – підтримка політики безпеки.	3
31.	Опишіть дискреційну політику безпеки.	3
32.	Опишіть переваги та недоліки дискреційної політики безпеки.	3
33.	Опишіть мандатну політику безпеки.	3
34.	Опишіть переваги та недоліки мандатної політики безпеки.	3
35.	Опишіть рольову політику безпеки.	3
36.	Опишіть політику безпеки - монітор безпеки.	4
		110

6.Методи та засоби діагностики результатів навчання:

– усне або письмове опитування;
– тестування;
– захист лабораторних робіт;
– екзамен.

7.Методи навчання:

- словесний метод (лекція);

- метод практико-орієнтованого навчання;
- робота з навчально-методичною літературою (конспектування, тезування, анотування);
- самостійна робота (опрацювання тем самостійної роботи).

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. **Концептуальні засади захисту інформації в автоматизованих системах.**		
Лабораторна робота 1.	ПРН2. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів. Практичні навички застосування сучасних технологій забезпечення інформаційної безпеки в системах автоматизації. ПРН3. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки, а також критичне осмислення сучасних проблем у сфері автоматизації та комп'ютерно-інтегрованих технологій для розв'язування складних задач професійної діяльності.	**25**
Лабораторна робота 2.		**20**
Лабораторна робота 3.		**25**
Лабораторна робота 4.		**20**
Модульна контрольна робота 1.		**10**
Всього за модулем 1		**100**
Модуль 2. ***Енергоефективне керування в цифрових інфокомунікаційних та електроенергетичних комп'ютерно-інтегрованих системах***		
Лабораторна робота 5.	ПРН2. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів. Уміння аналізувати системи на предмет захищеності та визначати нормативні документи в галузі захисту інформації в системах автоматизації, а також технічні методи захисту інформації. ПРН9. Розробляти функціональну, організаційну, технічну та інформаційну структури систем автоматизації складними технологічними та організаційнотехнічними об'єктами, розробляти програмно-технічні керуючі комплекси із застосовуванням мережевих та інформаційних технологій, промислових контролерів, мехатронних компонентів, робототехнічних пристроїв, засобів людино-машинного інтерфейсу та з урахуванням технологічних умов та вимог до управління виробництвом.	**25**
Лабораторна робота 6.		**20**
Лабораторна робота 7.		**20**
Лабораторна робота 8.		**25**
Модульна контрольна робота 2.		**10**
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*)	-	**-**

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). Курсові роботи 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=1306);
- конспекти лекцій та їх презентації (в електронному вигляді);
- підручники, навчальні посібники;
- методичні матеріали щодо вивчення навчальної дисципліни.

10.Рекомендовані джерела інформації

Основні:

1. Основи кіберпростору, кібербезпеки та кіберзахисту: навчальний посібник / В. М. Богуш [та ін.]. - К.: Ліра-К, 2020. - 554 с.

Допоміжні:

2. Проектування систем обробки та захисту інформації: навчальний посібник / О. М. Кулініч [та ін.]; Національний університет біоресурсів і природокористування України. - К.: ЦП "Компринт", 2023. - 415 с.

3. Організаційне забезпечення захисту інформації: навчальний посібник. Частина 1. Аудит інформаційної безпеки / В. А. Лахно [та ін.]; Національний університет біоресурсів і природокористування України. - К.: ЦП "Компринт", 2022. - 432 с.

4. Автоматизовані системи управління: навчальний посібник / В. В. Осипенко, М. О. Кіктєв, В. П. Лисенко. - К.: НУБіП України, 2018. - 668 с.

5. Автоматизований моніторинг сигналів синхронізації часу енергосистем: монографія / В.В. Коваль, О.В. Самков, І.В. Блінов, О.Л. Ламеко, І.В. Трач, С.Й. Поліщук, В.І. Вакась, В.В. Чопик, О.Л. Осінський, 2021. К.: Видавничий центр НУБіПУ, 2021. - 380 с.

6.Захист інформації в комп'ютерних системах і кібербезпека: навчальний посібник для самостійної роботи студентів ОС Магістр спеціальностей 123 - Комп'ютерна інженерія: ОПП - КсіМ, ОО - КСЗІ). Частина 1. Моделі і методи захисту інформаційно-комунікаційного середовища на основі інтелектуального розпізнавання загроз / В. А.

Лахно [та ін.]; Національний університет біоресурсів і природокористування України. - К.: Редакційно-видавничий відділ НУБіП України, 2023. - 301 с.
7. Інформаційна безпека: навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. Ю. Я. Бобала, І. В. Горбатого. – Львів: вид-во Львівської політехніки, 2019. – 580 с.
8.Якименко І.З. Менеджмент інформаційної безпеки: Конспект лекцій з дисципліни / Тернопіль – 2019. – 218 с.
9.Управління інформаційною безпекою: конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. - Київ: КПІ ім. Ігоря Сікорського, 2021. – 258 с.
10.Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / Уклад. Джулій В. М., Кльоц Ю. П., Муляр І. В., Чешун В.М. – Хмельницький: ХНУ, 2021. – 174с.
11.Даник Ю. Г. Основи кібербезпеки та кібероборони: підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – 2-ге вид., перероб. та доп. – Одеса : ОНАЗ ім. О.С. Попова, 2019. − 320 с.
12.Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс]: постанова КМУ від 19.06.2019 р., № 518.: офіц. вебсайт Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-п.
13.Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук’яненко В.В., ТПК «Орхідея», 2019. – 144 с.
14.Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни «Захист інформації та мережева безпека» для здобувачів вищої освіти першого (бакалаврського) рівня за освітньо-професійною програмою «Робототехніка та штучний інтелект» та «Автоматизація та комп’ютерно-інтегровані технології» спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» денної і заочної форм навчання [Електронне видання] / Наумчук О. М. – Рівне: НУВГП, 2023. –80 с.
15.Манжай О. В. Правові засади захисту інформації: підручник / О. В. Манжай, І.А, Манжай. – Харків: Панов, 2020. – 162 с.
16.НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу/ https://duikt.edu.ua/ru/lib/1/category/925/view/1021?lang=ru&act=view&page=1&category=925&id=1021
17.НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі.
18.Закон України «Про державну таємницю». – К.: Відомості Верховної Ради України, 1994. - N 16. - Ст. 93.
19.Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». – К.: Відомості Верховної Ради України, 1994. - N 31. - Ст. 286.
20.Закон України «Про інформацію». – К.:Відомості Верховної Ради України, 1992. - N 48. - Ст.650 .
21.Закон України «Про електронний цифровий підпис». – К.:Відомості Верховної Ради України, 2003. - N 36. - Ст.276 .
22.Hend K. Alkahtani. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions / Hend K. Alkahtani // Computer and Information Science. – Vol. 12, No. 2; 2019. – ISSN 1913-8989, E-ISSN 1913-8997. – Published by Canadian Center of Science and Education. – P. 117-125.
23.Муляр І.В. Модель оцінки ймовірнісно-часових характеристик інформаційної взаємодії в мережі інтернет речей / В.М. Джулій, Б.М. Кізюн, І.В. Муляр // Збірник наукових праць

Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. №63. – С. 51-60.

24. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions/ Hend K. Alkahtani. – Computer and Information Science. – Vol. 12, No. 2; 2019. – Published by Canadian Center of Science and Education. – P. 117-125. https://www.researchgate.net/publication/332779915_Safeguarding_the_Information_Systems_in_an_Organization_through_Different_Technologies_Policies_and_Actions/link/5cc9228992851c8d22105ad8/download

Інтернет-джерела:

1. http://nubip.edu.ua/ - головна сторінка НУБіП України.
2. http://nubip.edu.ua/node/1376 - кафедра автоматики та робототехнічних систем ім. акад. І.І.Мартиненка.
3. http://elibrary.nubip.edu.ua – електронна наукова бібліотека НУБіП України.
4. http://energ.nauu.kiev.ua/ - навчально-інформаційний портал ННІ енергетики, автоматики і енергозбереження.
5. https://duikt.edu.ua/ru/lib/1/category/925/view/1021?lang=ru&act=view&page=1&category=925&id=1021
6. https://elearn.nubip.edu.ua/course/view.php?id=1306