НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

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

"ЗАТВЕРДЖУЮ"
Директор ННІ енергетики,
автоматики і енергозбереження
(Каплун В.В.)
"____" _____ 2024 р.

"СХВАЛЕНО"
на засіданні кафедри
автоматики та робототехнічних
систем ім. акад. І.І. Мартиненка
Протокол №37 від "21" травня 2024 р.
Завідувач кафедри
(Лисенко В.П.)

"РОЗГЛЯНУТО"
Гарант ОНП підготовки магістрів
спеціальності 174 Автоматизація,
комп'ютерно-інтегровані
технології та робототехніка
Гарант ОП
(Коваль В.В.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ АВТОМАТИЗАЦІЇ

Галузь знань 17 Електроніка, автоматизація та електронні комунікації
Спеціальність 174 Автоматизація,комп'ютерно-інтегровані технології та робототехніка
Освітня програма Автоматизація, комп'ютерно-інтегровані технології та робототехніка
Факультет (ННІ) ННІ енергетики, автоматики і енергозбереження
Розробники: професор, докт. техн. наук, професор Коваль Валерій Вікторович
(посада, науковий ступінь, вчене звання)

Київ – 2024 р.

Опис навчальної дисципліни "Захист інформації в системах автоматизації"
(назва)

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*магістр*	
Спеціальність	*174 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 (2024/2025)	
Семестр	2	
Лекційні заняття	*20 год.*	*год.*
Практичні, семінарські заняття	*год.*	*год.*
Лабораторні заняття	*20год.*	*год.*
Самостійна робота	*110 год.*	*год.*
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	*4 год.*	

1.**Мета, завдання, 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.

Завдання – 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.

Набуття компетентностей:

інтегральна компетентність (ІК): Здатність розв'язувати складні задачі і проблеми автоматизації та комп'ютерно-інтегровних технологій у професійній діяльності та/або у процесі навчання, що передбачає проведення досліджень та/або провадження інноваційної діяльності та характеризується комплексністю та невизначеністю умов і 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 для:**

– повного терміну денної форми здобуття вищої освіти.

Назви змістових модулів і тем	Кількість годин						
	денна форма						
	тижні	усього	у тому числі				
			л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8
Змістовий модуль 1. ***Концепція захисту інформації в автоматизованих системах.***							
Тема 1. Предмет та об'єкт захисту у інформаційній безпеці. Комп'ютерні системи і мережі.	23	15	2		2		11
Тема 2. Проблеми захищеності цифрових сигналів керування в системах автоматизації Взаємодія відкритих систем. Інформаційна безпека протоколів. IP-протокол та атаки, пов'язані з адресацією.	24	15	2		2		11
Тема 3. Загрози безпеці інформації. Поняття та класифікація загроз інформації в автоматизованих системах. Характеристика загроз безпеки інформації. Несанкціонований доступ.	25	15	2		2		11
Тема 4. Технічні канали витоку інформації. Поняття порушника інформаційної безпеки. Модель	26	15	2		2		11

порушника.							
Тема 5. Концепція захисту інформації. Шляхи забезпечення безпеки інформації. Політика безпеки інформації.	27	15	2		2		11
Разом за змістовим модулем 1		75	10		10		55
Змістовий модуль 2. ***Комплексний захист інформації автоматизованих систем.***							
Тема 1. Забезпечення комплексності вирішення завдань інформаційної безпеки. Діяльність міжнародних організацій, що діють у сфері інформаційної безпеки.	28	15	2		2		11
Тема 2. Міжнародні стандарти проєктування та експлуатації систем автоматизації. Стандартизація в сфері менеджменту інформаційної безпеки. Стандарти IEC/ISA 62443 для підтримки безпечної експлуатації промислових систем автоматизації.	29	15	2		2		11
Тема 3. Концепція, стратегія та архітектура захисту інформації. Етапи розробки. Політика захисту інформації.	30	15	2		2		11
Тема 4. Управління ризиками. Загрози,	31	15	2		2		11

прогнозування та оцінка їх наслідків. Ризик-менеджмент.							
Тема 5. Етапи створення комплексної системи захисту інформації (КСЗІ). Державна експертиза КСЗІ та супровід в період функціонування.	32	15	2		2		11
Разом за змістовим модулем 2		75	10		10		55
Усього годин	150		20		20		110
Курсовий проект (робота) з _____ _____ _ (якщо є в робочому навчальному плані)			-	-	-		-
Усього годин	150		20		20		110

3.**Теми лабораторних занять**

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

7	Дослідження генератора псевдовипадкової послідовності, скремблера та дескремблера кіберінформації систем автоматизації.	3
8	Аналіз стандартів IEC/ISA 62443 для підтримки безпечної експлуатації промислових систем автоматизації.	3

4.**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.	4
4.	Наведіть особливості теорії захисту інформації.	3
5.	Вкажіть у чому полягають формальні та неформальні підходи до розгляду питань теорії захисту інформації.	3
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.	3
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.	3
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.	3
		110

5.Засоби діагностики результатів навчання:

- екзамен;
- модульні тести;
- захист лабораторних робіт.

6.**Методи навчання:**

- словесний метод (лекція);
- практичний метод (лабораторні заняття);
- наочний метод (метод ілюстрацій, метод демонстрацій);
- робота з навчально-методичною літературою (конспектування, тезування, анотування);
- відеометод (дистанційні, мультимедійні, веб-орієнтовані);
- самостійна робота (опрацювання тем самостійної роботи).

7.Методи оцінювання.

- екзамен;
- усне або письмове опитування;
- модульне тестування;
- захист лабораторних робіт.

8.Розподіл балів, які отримують здобувачі вищої освіти. Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 чинного «Положення про екзамени та заліки у НУБіП України»

Рейтинг здобувача вищої освіти, бали	Оцінка національна та результати складання	
	екзаменів	заліків
90-100	відмінно	зараховано
74-89	добре	
60-73	задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу здобувача вищої освіти із засвоєння дисципліни $\mathbf{R_{ДИС}}$ (до 100 балів) одержаний рейтинг з атестації (до 30 балів) додається до рейтингу здобувача вищої освіти з навчальної роботи $\mathbf{R_{НР}}$ (до 70 балів): $\mathbf{R_{ДИС} = R_{НР} + R_{АТ}}$.

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

Електронні ресурси:

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
7. https://elearn.nubip.edu.ua/course/view.php?id=1306