СИЛАБУС ДИСЦИПЛІНИ
«Захист інформації в системах автоматизації»

Ступінь вищої освіти - Магістр
Спеціальність 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
Освітня програма «Автоматизація, комп'ютерно-інтегровані технології та робототехніка**»**
Рік навчання 2024/2025, семестр 2
Форма здобуття вищої освіти денна
Кількість кредитів ЄКТС 4
Мова викладання українська

Лектор навчальної дисципліни	**проф. Коваль Валерій Вікторович**
Контактна інформація лектора (e-mail)	**(096) 424-88-32, v.koval@nubip.edu.ua**
URL ЕНК на навчальному порталі НУБіП України	**https://elearn.nubip.edu.ua/course/view.php?id=4128**

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

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

Компетентності навчальної дисципліни:

інтегральна компетентність (ІК): Здатність розв'язувати складні задачі і проблеми автоматизації та комп'ютерно-інтегрованих 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.

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.

Програмні результати навчання навчальної дисципліни: ПРН2. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема	**Години** (лекції/ лабораторні, практичні, семінарські, самостійна)	Результати навчання	Завдання	Оцінювання
Модуль 1 Концепція захисту інформації в автоматизованих системах				
Тема1 Предмет та об'єкт захисту у інформаційній безпеці. Комп'ютерні системи і мережі.	2/2/5	Знати загальні положення теорії захисту інформації, класифікацію загроз інформації та вміти формулювати загальну постановку задачі захисту інформації в комп'ютерних і автоматизованих системах.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	20

Тема 2 Проблеми захищеності цифрових сигналів керування в системах автоматизації.	0/2/5	Знати загальну характеристику сучасних систем обробки інформації, особливості захищеності цифрових сигналів керування в системах автоматизації. Вміти при розробці автоматизованих систем визначати предмет та об’єкт захисту у інформаційній безпеці.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	20
Тема 3 Взаємодія відкритих систем. Інформаційна безпека протоколів. IP-протокол та атаки, пов'язані з адресацією.	2/2/5	Знати типові рівні інформаційно-комунікаційних систем, способи комутації, IP-протоколи та атаки, пов'язані з адресацією. Вміти при використанні інформаційно-комунікаційних систем визначати особливості IP-протоколів для зменшення ризику загроз.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	20
Тема 4 Загрози безпеці інформації. Поняття та класифікація загроз інформації в автоматизованих системах.	0/2/5	Знати профілі захищеності інформаційних систем, характеристики загроз безпеки інформації та типові атаки на інформаційний ресурс. Вміти виконувати класифікацію загроз інформації в автоматизованих системах.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn)..	20
Тема 5 Характеристика загроз безпеки інформації. Несанкціонований доступ.	2/2/5	Знати види і типи загроз безпеки інформації. Вміти визначати загрози цілісності інформації та доступності в автоматизованих системах.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	10
Тема 6 Технічні канали витоку інформації. Поняття порушника інформаційної безпеки. Модель порушника.	0/2/5	Знати технічні канали витоку інформації та моделі каналу витоку інформації, моделі порушників безпеки інформації. Вміти використовувати ці моделі для комплексного захисту інформації в автоматизованих системах.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	10
Тема 7 Концепція захисту інформації. Шляхи забезпечення безпеки інформації. Політика	1/3/5	Знати концепцію захисту інформації, як методологічну основу політики розробки практичних заходів для її реалізації. Вміти використовувати концепцію захисту інформації в автоматизованих системах.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	10

безпеки інформації.				
Тест			**Написання тестів**	10
Модуль 2. Комплексний захист інформації автоматизованих систем				
Тема 1 Організаційне забезпечення інформаційної безпеки. Забезпечення комплексності вирішення завдань інформаційної безпеки.	2/1/5	Знати основні напрямки роботи в загальній системі заходів у сфері інформаційної безпеки. Вміти виявляти всі значущі інформаційні об'єкт, а також існуючі і потенційно можливі загрози і на основі цього забезпечувати комплексне впровадження і застосування засобів захисту інформації.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	20
Тема 2 Діяльність міжнародних організацій, що діють у сфері інформаційної безпеки (ITU, IEEE, ISO, NIST).	0/2/5	Знати міжнародні організації, що діють у сфері інформаційної безпеки. Вміти використовувати стандарти та рекомендації для захисту інформації в системах автоматизації.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	20
Тема 3 Міжнародні стандарти проєктування та експлуатації систем автоматизації. Стандартизація в сфері менеджменту інформаційної безпеки.	2/2/5	Знати діючі стандарти з проєктування, експлуатації систем автоматизації та захисту інформації. Вміти знаходити стандарти, що стосуються технічних рішень по архітектурі, алгоритмам, протоколам загальнодоступним засобам шифрування даних, правилам побудови глобальних мереж обміну даними та інших елементів глобальної інфраструктури інформаційної безпеки.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	20
Тема 4 Стандарти IEC/ISA 62443 для підтримки безпечної експлуатації промислових систем автоматизації.	0/2/5	Знати стандарти і технічні звіти серії IEC/ISA 62443 для підтримки безпечної експлуатації промислових систем автоматизації. Вміти використовувати стандарти серії IEC/ISA 62443 для протидії комп'ютерним злочинам та захисту інформації в промислових системах автоматизації.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	20

Тема 5 Концепція, стратегія та архітектура захисту інформації. Етапи розробки. Політика захисту інформації.	2/2/5	Знати офіційно прийняту систему поглядів на проблему інформаційної безпеки та шляхи її рішення з урахуванням сучасних тенденцій. Вміти розробляти документ, де перераховуються правила доступу, визначаються шляхи реалізації політики та описується базова архітектура середовища захисту..	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	10
Тема 6 Управління ризиками. Загрози, прогнозування та оцінка їх наслідків. Ризик-менеджмент.	0/2/5	Знати нормативну та правову бази з питань організації та проведення аудиту інформаційної безпеки, методик оцінки інформаційних ризиків. Вміти розробляти комплекс заходів, спрямованих на впровадження інформаційних технологій, які забезпечують обробку інформації згідно з нормативними документами у сфері захисту інформації.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	10
Тема 7 Етапи створення комплексної системи захисту інформації (КСЗІ).	2/2/5	Знати нормативно-правові акти України, які визначають необхідність створення КСЗІ. Вміти визначити етапи та види захисту від загроз для інформаційних ресурсів, які циклічно повторюються з метою постійного оновлення та підвищення ефективності заходів і засобів захисту.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	10
Тема 8 Державна експертиза КСЗІ та супровід в період функціонування.	0/2/5	Знати нормативно-правові документи, які необхідно виконувати в процесі державної експертизи КСЗІ. Вміти виконувати заходи, які здійснюються під час супроводу КСЗІ.	Виконання лабораторної роботи. Виконання самостійної роботи (в.т.ч. в elearn).	10
Тест			**Написання тестів**	10
Всього за семестр				**70**
Екзамен				**30**
Всього за курс				**100**

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). Видавати чужі результати лабораторних робіт за власні. Курсові роботи, реферати повинні мати коректні текстові посилання на використану літературу
Політика щодо відвідування:	Відвідування занять є обов'язковим, окрім навчання за індивідуальними планами. При оформленні індивідуального плану навчання відвідування лекційних занять на розсуд студента, за можливості виконання лабораторних робіт на власному обладнанні вони можуть робитись поза університетом проте захист має бути персональним. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в он-лайн формі за погодженням із Дирекцією ННІ)

ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

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

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні:

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

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.

Допоміжні:

1. 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.

2. 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.

3. Захист інформації: конспект лекцій, лабораторних і практичних робіт для студ. спец. 6.050101 "Комп'ютерні науки" / Б. В. Кузьменко, В. П. Лисенко, М. В. Андріїшина, М. В. Чапний; Національний університет біоресурсів і природокористування України (К.). - К.: [б. и.], 2009. - 191 с.

4. 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.

5. Якименко І.З. Менеджмент інформаційної безпеки: Конспект лекцій з дисципліни / Тернопіль – 2019. – 218 с.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. Манжай О. В. Правові засади захисту інформації: підручник / О. В. Манжай, І.А, Манжай. – Харків: Панов, 2020. – 162 с.

13. 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

14. НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі.

15. Закон України «Про державну таємницю». – К.: Відомості Верховної Ради України, 1994. - N 16. - Ст. 93.

16. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». – К.: Відомості Верховної Ради України, 1994. - N 31. - Ст. 286.

17. Закон України «Про інформацію». – К.:Відомості Верховної Ради України, 1992. - N 48. - Ст.650 .

18. Закон України «Про електронний цифровий підпис». – К.:Відомості Верховної Ради України, 2003. - N 36. - Ст.276 .

19. 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.

20. 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.

21. 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