ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра автоматизації та комп'ютерно-інтегрованих технологій

ЗАТВЕРДЖУЮ
Декан ФІТС _____ Олег САВЕНКО
01.09. 2022 р.

СИЛАБУС

Навчальна дисципліна **Функціональна та кібербезпека систем автоматизації**

Освітньо-наукова програма **Автоматизація та комп'ютерно-інтегровані технології**

Рівень вищої освіти **другий (магістерський)**

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	**Савенко Олег Станіславович** **Корецька Людмила Олександрівна**
Профайл викладача	http://kiis.khmnu.edu.ua/personnel/savenko-oleg-stanislavovych/ http://kiis.khmnu.edu.ua/personnel/koreczka-kovtun-lyudmyla-oleksandrivna/
E-mail викладача(ів)	savenko_oleg_st@ukr.net koretskal@khmnu.edu.ua
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=7973
Навчальний рік	2022-2023
Консультації	**Очні**: середа, 13.00-14.30, ауд.1-115; **онлайн:** за необхідністю та попередньою домовленістю

Характеристика дисципліни

Статус дисципліни	Форма навчання	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
						Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС				
				Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
О	Д	1	2	5	150	54	18	36			96				+

Анотація дисципліни

Дисципліна "Функціональна та кібербезпека систем автоматизації" є однією з дисциплін загальної підготовки магістрів автоматизації та комп'ютерно-інтегрованих технологій.

Дисципліна викладається для здобувачів другого (магістерського) рівня вищої освіти денної форми навчання спеціальностей галузі автоматизації та приладобудування. При викладанні дисципліни використовуються активні і творчі форми проведення занять, зокрема, методи проблемного навчання.

Мета і завдання дисципліни

Метою дисципліни "Функціональна та кібербезпека систем автоматизації" є:) формування компетентностей, необхідних для розроблення надійних систем автоматизації; 2) Ознайомити студентів із основними напрямками по забезпеченню функціональної та кібербезпеки систем автоматизації; 3) ознайомити студентів з теоретичною базою, що використовується при вирішенні задач оцінювання надійності систем автоматизації.

Завдання дисципліни. Надати студентам знання і практичні навички з оцінювання надійності автоматизованих систем; підготувати студентів до ініціювання та автономного провадження дослідницької та інноваційної діяльності в галузі функціональної та кібербезпеки систем автоматизації.

Пререквізити: Теорія, моделювання і оптимізація інтелектуальних і складних систем керування; Робототехнічні та інтелектуальні мехатронні пристрої і системи.

Кореквізити: Професійна практика.

Очікувані результати навчання

Після вивчення дисципліни "Функціональна та кібербезпека систем автоматизації" студент має досягти таких результатів навчання (сукупність знань, умінь, навичок, компетентностей):

Компетентності, на формування яких спрямовано ОК:

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.

ЗК4. Здатність працювати в міжнародному контексті.

ФК2. Здатність проєктувати та впроваджувати високонадійні системи автоматизації та їх прикладне програмне забезпечення, для реалізації функцій управління та опрацювання інформації, здійснювати захист прав інтелектуальної власності на нові проєктні та інженерні рішення

ФК3. Здатність застосовувати методи моделювання та оптимізації для дослідження та підвищення ефективності систем і процесів керування складними технологічними та організаційно-технічними об'єктами.

ФК4. Здатність аналізувати виробничо-технологічні системи і комплекси як об'єкти автоматизації, визначати способи та стратегії їх автоматизації та цифрової трансформації.

ФК8. Здатність розробляти функціональну, технічну та інформаційну структуру комп'ютерно-інтегрованих систем управління організаційно-технологічними комплексами із застосуванням мережевих та інформаційних технологій, програмно-технічних керуючих комплексів, промислових контролерів, мехатронних компонентів, робототехнічних пристроїв та засобів людино-машинного інтерфейсу.

ФК12. Здатність застосовувати новітні комп'ютерно-інтегровані технології для забезпечення функціональної та кібербезпеки систем автоматизації.

Програмні результати навчання, на забезпечення яких спрямовано ОК:

ПРН2. Створювати високонадійні системи автоматизації з високим рівнем функціональної та інформаційної безпеки програмних та технічних засобів.

ПРН4. Застосовувати сучасні підходи і методи моделювання та оптимізації для дослідження та створення ефективних систем автоматизації складними технологічними та організаційно-технічними об'єктами.

ПРН5. Розробляти комп'ютерно-інтегровані системи управління складними технологічними та організаційно-технічними об'єктами, застосовуючи системний підхід із врахуванням нетехнічних складових оцінки об'єктів автоматизації.

ПРН9. Розробляти функціональну, організаційну, технічну та інформаційну структури систем автоматизації складними технологічними та організаційно-технічними 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.

ПРН10. Розробляти і використовувати спеціалізоване програмне забезпечення та цифрові технології для створення систем автоматизації складними організаційно-технічними об'єктами, професійно володіти спеціальними програмними засобами.

ПРН12. Збирати необхідну інформацію, використовуючи науково-технічну літературу, бази даних та інші джерела, аналізувати і оцінювати її.

ПРН16. Розробляти і використовувати пристрої функціональної безпеки на основі програмованих і мережевих системи безпеки.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лабораторної роботи*	Самостійна робота студентів		
			Зміст	Год.	Література
1-2	Функціональна безпека: основні поняття та визначення	Оцінка потенційної небезпеки виробничих процесів	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи №1.	11	[2-5, 7]
3-4	Функціональна безпека та «Інтернет-речей» у промисловості	Резервування у системах автоматизації: модулі введення, давачі	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №1. Підготовка до лабораторної роботи №2.	11	[2-5, 7]
5-6	Вимоги до інформаційної безпеки	Резервування у системах автоматизації: модулі виведення	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №2. Підготовка до лабораторної роботи №3.	11	[8, 9]
7-8	Методи забезпечення функціональної безпеки	Резервування у системах автоматизації: процесорні модулі	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №3. Підготовка до лабораторної роботи №4.	11	[2-5, 7]
9-10	Резервування у автоматизованих системах управління	Резервування у системах автоматизації: джерела живлення	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №4. Підготовка до лабораторної роботи №5.	11	[5-7]
11-12	Відповідність вимогам інформаційної та функціональної безпеки за допомогою методології Assurance Case	Оцінка надійності систем автоматизації із резервуванням	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №5. Підготовка до лабораторної роботи №6.	11	[8, 9]
13-14	Комплексні системи захисту інформації в системі забезпечення функціональної безпеки АСУ		Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №6. Підготовка до лабораторної роботи №7.	11	[8-11]
15-16	Кібербезпека в АСУ ТП	Використання програмного забезпечення YARA для виявлення шкідливого програмного забезпечення	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №7. Підготовка до лабораторної роботи №8.	11	[8-11]
17-18	Підсумкове заняття	Налаштування міжмережевого екрану у операційній системі Windows	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи №8. Підготовка до підсумкового контрольного заходу.	8	

Примітка: * Послідовність проведення занять визначається розкладом (може не відповідати нумерованим тижням)

Політика дисципліни

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, практичні заняття згідно з розкладом, не запізнюватися на заняття, завдання виконувати відповідно до графіка. До практичних занять студент має підготуватися за відповідною темою і проявляти активність. Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання у ХНУ. Як результати навчання, отримані у неформальній освіті, зокрема онлайн-курси «IoT Fundamentals: IoT Security» (https://www.netacad.com/courses/cybersecurity/iot-security) може бути зараховано виконання двох лабораторних робіт: №7, №8.

Критерії оцінювання результатів навчання.

Кожний вид роботи з дисципліни оцінюється за ***чотирибальною*** шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з врахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих її видів робіт. При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на її початку; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи згідно з робочою програмою дисципліни і робочим навчальним планом.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів денної форми навчання у семестрі за ваговими коефіцієнтами

Аудиторна робота	Семестр. контроль (іспит)
Лабораторні роботи №:	Підсумковий контрольний захід
1-8	
ВК: 0,6	0,4

Умовні позначення: ВК – ваговий коефіцієнт.

Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ECTS	**Інституційна шкала балів**	**Інституційна оцінка**		**Критерії оцінювання**
A	4,75-5,00	5	Зараховано	**Відмінно** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків.
B	4,25-4,74	4		**Добре** – повне знання навчального матеріалу з кількома незначними помилками.
C	3,75-4,24	4		**Добре** – в загальному правильна відповідь з двома-трьома суттєвими помилками.
D	3,25-3,74	3		**Задовільно** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією.
E	3.00-3,24	3		**Задовільно** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00-2,99	2	Незараховано	**Незадовільно** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00-1,99	2		**Незадовільно** – необхідна серйозна подальша робота і повторне вивчення дисципліни.

Питання для підсумкового контролю з дисципліни

1. Основні протоколи передачі даних та автентифікації, які використовуються в «Автоматизованих системах».
2. Основні поняття у сфері функціональної безпеки.
3. Основні засоби забезпечення функціональної безпеки (архітектура, принципи побудови).
4. Принципи проектування систем безпеки об'єктів автоматизації.
5. Класифікація та приклади систем автоматизації, приклади загроз, уразливостей, ризиків.
6. Основні ризики та проблеми функціональної безпеки систем автоматизації.
7. Рівні безпеки SIL.
8. Атрибути надійності, інформаційної та функціональної безпеки.
9. Структурні схеми надійності.
10. Поняття дерева відмови.
11. Аналіз видів, наслідків та критичності відмов (ЄМЕСА).
12. Як виглядає модель відмов із загальної причини
13. Методи резервування в АСУ ТП
14. Основні принципи резервування
15. Резервування нижнього рівня АСУ ТП.
16. Резервування середнього рівня АСУ ТП.
17. Резервування верхнього рівня АСУ ТП.
18. Резервування промислових мереж

19. Протоколи резервування
20. Оцінка надійності резервованих систем
21. Організація підтримки забезпечення функціональної безпеки в системах SCADA.
22. Дублювання функцій.
23. Розмежування прав доступу в системах функціональної безпеки (оператор, головний оператор, системи автоматичного контролю).
24. Системи реального часу в АСУ ТП.
25. Організація систем реального часу в АСУ ТП.
26. Архітектура систем реального часу
27. Стандарти функціональної безпеки.
28. Життєвий цикл функціональної безпеки.
29. Структура життєвого циклу інформаційної та функціональної безпеки
30. Технічні методи забезпечення функціональної безпеки.
31. Методи захисту від відмов апаратних засобів та систем відповідно до вимог.
32. Методи захисту від програмних відмов, забезпечення відповідно до вимог.
33. Структура вимог щодо інформаційної безпеки
34. Особливості забезпечення інформаційної безпеки комп'ютерних систем керування
35. Основні ризики та проблеми кібербезпеки в промисловому Інтернеті речей.
36. Основні поняття в галузі кібербезпеки АСУ ТП та Інтернету речей.
37. Основні загрози, ризики та вразливості у сфері кібербезпеки АСУ ТП та критичної інформаційної інфраструктури.
38. Основні протоколи передачі даних та аутентифікації, що використовуються в АСУ
39. Технологічний процес та Інтернет речей.
40. Основні визначення системи забезпечення інформаційної безпеки та особливості побудови системи забезпечення інформаційної безпеки для об'єктів критичної інформаційної інфраструктури на промислових об'єктах.
41. Основні засоби забезпечення кібербезпеки (архітектура, принципи побудови).
42. Принципи проектування безпечної інфраструктури об'єктів АСУ ТП.
43. Основні ризики та проблеми кібербезпеки АСУ ТП.
44. Критерії оцінки безпеки, основних загроз, ризиків та проблем, структури та особливостей побудови моделі загроз.
45. Методи та засоби забезпечення безпеки мережної інфраструктури об'єктів АСУ ТП.
46. Приклади інцидентів інформаційної безпеки в АСУ ТП (kill-chain, скомпрометована інфраструктура, наслідки).
47. Методи забезпечення безпеки інформації при аваріях.
48. Захист інформації АСУ ТП від несанкціонованого доступу.
49. Методи безпечного управління змінами у ПЗ та мережному обладнанні об'єктів АСУ ТП.
50. Різниця між кібератакою та кіберфізичною атакою.
51. Протоколы связи и аутентификации для киберфизических систем и «Интернет-вещей»
52. Класифікація видів кібератак на промислові та IoT системи
53. Вразливості існуючих промислових мереж та використовуваних протоколів
54. Можливі сценарії атак, оцінка ризиків для АСУ ТП

Методичне забезпечення

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі.

Рекомендована література

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163–VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 07.08.2022р.).

2. IEC TS 61508-3-1:2016. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3-1: Software requirements - Reuse of pre-existing software elements to implement all or part of a safety function [Publication date:2016-07-13]. IEC, 2016. 10p.

3. IEC TR 61508-0:2005. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 0: Functional safety and IEC 61508 [Publication date: 2005-01-20]. IEC, 2005. 33p.

4. IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems [Publication date: 2010-04-30]. IEC, 2010.

5. Карташов В.В. Автоматизовані системи керування технологічними процесами : посібник з лекцій. Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2017. 149 с.

6. Розрахунки систем контролю та керування : навчальний посібник / Манко Г.І. та ін. Дніпро : УДХТУ, 2018. 191 с.

7. Автоматизація виробничих процесів: підручник / Ельперін І.В., Пупена О.М., Сідлецький В.М., Швед С.М. К : Видавництво Ліра-К, 2015. 378 с.

8. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки : навчальний посібник. Вінниця : ВНТУ, 2018. 316 с.

9. Хорошко В. О., Орєхова І. І., Яремчук Ю. Є. Основи науково-дослідної роботи в галузі інформаційної безпеки : навчальний посібник. Київ : ДУІКТ, 2012. 175 с.

10. Основи криптографічного захисту інформації / Гулак Г. М., Мухачов В. А., Хорошко В. О., Яремчук Ю. Є. Вінниця : ВНТУ, 2011. 199 с.

11. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К. : ДУТ, 2015. 288 с.

12. Васильківський І. С., Федінець В. О., Юсик Я. П. Виконавчі пристрої систем автоматизації. Львів: Львівська політехніка, 2020. 220 с.

13. Rausand M. Reliability of safety-critical systems : theory and application. Wiley, 2013. P. 468.

14. Савенко О., Корецька Л., Хома Д. Підвищення функціональної безпеки протипожежного контуру автоматизованої системи. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2022. №2. С. 88-95

15. Lysenko, S.; Bobrovnikova, K.; Kharchenko, V.; Savenko, O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. *Algorithms* 2022, 15, 239. https://doi.org/10.3390/a15070239

16. Nattawadee Thiemthummawong, Arjin Numsomran, Vittaya Tipsuwanpor, Twitch Chumuang. PFDavg Calculation based on Minimal Cut Set with Safety Condition. *Proceedings of the World Congress on Engineering and Computer Science*. 2017. October 25-27. Vol. I.

Розробники: д.т.н., професор Олег САВЕНКО

к.т.н., доцент Людмила КОРЕЦЬКА

Погоджено:

Зав. каф. АКІТ д.т.н., професор Валерій МАРТИНЮК

Гарант ОП д.т.н., професор Валерій МАРТИНЮК