Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№503)

ЗАТВЕРДЖУЮ

Голова НМК
_____ Д.М. Крицький
(підпис) (ініціали та прізвище)

«_31_» __08_____ 2022 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи дослідження комп'ютерних систем та мереж
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 123 «Комп'ютерна інженерія»
(код та найменування спеціальності)

Освітня програма: «Комп'ютерні системи і мережі»
(найменування освітньої програми)

Освітня програма: «Системне програмування»
(найменування освітньої програми)

Освітня програма: «Програмовні мобільні системи і інтернет речей»

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2022 рік

Робоча програма «Методи дослідження комп'ютерних систем та мереж”:
(назва навчальної дисципліни)

Розробники: Брежнєв Є. В., професор кафедри 503 д.т.н, проф..
(автор, посада, науковий ступень та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп’ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2022 р.

Завідувач кафедри д.т.н., професор В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 4.0</td><td rowspan="11">Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 8.123 (Комп’ютерні системи та мережі)
(шифр і назва галузі знань)

Освітня програма:
«Комп’ютерні системи та мережі»
«Системне програмування»

«Програмовні мобільні системи і інтернет речей»

Рівень вищої освіти:
освітньо-науковий
другий (магістерський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 3</td><td rowspan="2">Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – не має</td></tr>
<tr><td>Індивідуальне завдання: немає</td><td>2022/2023</td></tr>
<tr><td>Загальна кількість годин – 48/120</td><td rowspan="2">Семестр: 2
(магістри)</td></tr>
<tr><td rowspan="9">Кількість тижневих годин для денної форми навчання:
аудиторних – 2

практичні роботи – 2 (через тиждень)</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td>32 год.</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>16 год.</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>0 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>72 год.</td></tr>
<tr><td>Вид контролю:</td></tr>
<tr><td></td><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *48/72*.

* Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: є отримання магістрами теоретичних знань і навичок зі дослідження складних енергетичних інфраструктур (КЕІ) та інформаційно-керуючих систем (ІКС), методів керування КЕІ та проектного менеджменту ІКС, дослідження ефективності складних систем, застосування інформаційних технологій при вирішенні відповідних завдань з управління.

Завдання: є вивчення базових понять з дослідження складних систем, мереж, оцінювання ефективності, якості життєвого циклу КЕІ та ІКС, антикризового та проектного менеджменту КЕІ, системного аналізу, що потрібного враховувати при створенні КЕІ.

Згідно з вимогами освітньо-професійної програми и повинні досягти таких **компетентностей:**

1. **Загальні:**

ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.
ЗК3. Здатність проводити дослідження на відповідному рівні.
ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК5. Здатність генерувати нові ідеї (креативність).
ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
ЗК7. Здатність приймати обґрунтовані рішення.

2. Фахові**:**

СК4. Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.
СК7. Здатність досліджувати, розробляти та обирати технології створення великих і надвеликих систем.
СК8. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.
СК11.Здатність обирати ефективні методи розв'язування складних задач комп'ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення.
СК12. Здатність використовувати методи аналізу, ідентифікації й синтезу комп'ютерних систем та мереж, кіберфізичних систем, засобів Інтернету речей та ІТ-інфраструктур.

Результати навчання: вміти застосовувати методи та інструментальні засоби дослідження КЕІ та ІКС, методів антикризового та проектного менеджменту КЕІ та ІКС. Мати навички з застосування цих методів при вирішенні практичних завдань.

Міждисциплінарні зв'язки: В частині вивчення структур даних дисципліна базується на деяких поняттях дисципліни «Теорія і методи зеленої ІТ-інженерії», а також на поняттях дисципліни «Теорія і технології критичного комп'ютингу», «Методи та технології кібербезпеки критичних інфраструктур».

3. Програма навчальної дисципліни

Модуль 1. Вступ до дисципліни.

Тема 1 Складні енергетичні інфраструктури та інформаційно-керуючі системи (ІКС) як об'єкти дослідження. Основні питання з дослідження складних КС та їх безпеки. Основні визначення, класифікація, загрози, вразливості. Основні положення "Зеленої книги з захисту критичної інфраструктури". Дослідження резіліенсу складних систем. Основні поняття захисту критичної інформаційної інфраструктури. Основні поняття ризик аналізу. Архітектура КЕІ та її мереж.

Тема 2 Основні поняття з дослідження складних систем на життєвому циклу. Життєвий цикл складних соціотехнічних систем. Каскадна, етапна, спіральна моделі життєвого циклу. Основні переваги та недоліки моделей життєвого циклу. Критерій оптимальності функціонування КЕІ. Визначення вимог до КЕІ. Життєвий цикл організації. Основні характеристики етапів. Моделі життєвого циклу організацій. Життєвий цикл ІТ продукту.

Тема 3 Аспекти системного підходу при дослідженні складних КС. Загальні принципи системного підходу при дослідженні КЕІ та ІКС. Основні властивості КЕІ та ІКС. Основні показники ефективності КЕІ та ІКС.

ЛР.

Огляд основних моделей життєвого циклу КЕІ та ІКС.

Вивчення стандарту ІСО/МЕК 15288-2005. Інформаційна технологія. Системна інженерія. Процеси життєвого циклу систем.

Модуль 2. Дослідження КЕІ за допомогою методів та інструментальних засобів.

Тема 4. Дослідження методів антикризового менеджменту складних КС. Основні методи антикризового менеджменту КЕІ. Принципи антикризового менеджменту. Класифікація кризисних явищ в організації. Методи та стратегії антикризового менеджменту. Інструментальні засоби та інформаційні технології антикризового менеджменту КЕІ.

Тема 5. Методи менеджменту ЖЦ при проектуванні та дослідженні складних КС. Основні методи управління та дослідження КС на ЖЦ. Підходи щодо керування ризиками, людськими ресурсами, комунікаціями, якістю при виконанні проекту зі створення ІКС. Управління змістом проекту (Project Scope Management). Управління термінами проекту (Project Time Management). Управління зацікавленими сторонами проекту (Project Stakeholder Management).

ЛР.

Огляд основних моделей діагностики кризису в КЕІ (моніторинг зовнішнього середовища КЕІ, аналіз дії конкурентів, аналіз ризиків).

Вивчення стандарту ISO 22301 Security and resilience — Business continuity management systems — Requirements.

Модуль 3. Дослідження основних фреймворків розробки КЕІ та ІКС.

Тема 6. Основні методології та фреймворки з розробки КЕІ та ІКС. Основні положення System of Systems Engineering в контексті дослідження складних систем. Вивчення AGILE, SCRUM, RAD, XP. Загальні принципи AGILE, SCRUM, RAD, XP. Етапи AGILE, SCRUM, RAD, XP. Переваги та недоліки кожного з фреймворків . Особливості застосування при проектуванні КЕІ та ІКС.

Тема 7. Апаратно-програмні платформи створення складних КС. Дослідження основних платформ створення ІКС АЕС. Визначення переваг та недоліків. Основні стандарти зі створення ІКС АЕС.

ЛР.

Порівняльний аналіз AGILE, SCRUM, RAD, XP.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	лаб.	п.	с.р.
1	2	3	4	5	6
Модуль 1. Вступ до дисципліни					
Тема 1. Основи дослідження складних систем на прикладі КЕІ та інформаційно-керуючі системи (ІКС).	12	4	8	-	-
Тема 2. Основні етапи життєвого циклу КЕІ та ІКС.	18	4	-	-	14
Тема 3. Аспекти системного підходу при створенні та досліджені КЕІ та ІКС.	14	4	-	-	10
Разом за модулем 1	**44**	**12**	**8**	**-**	**24**
Модуль 2. Дослідження КЕІ за допомогою методів та інструментальних засобів					
Тема 4. Методи антікризисного менежменту КЕІ.	18	4	4	-	10

Тема 5. Методи менеджменту ЖЦ при проектуванні КЕІ та ІКС	22	4	4	-	14
Разом за модулем 2	**40**	**8**	**8**	**-**	**24**
Модуль 3. Дослідження основних фреймворків розробки КЕІ та ІКС					
Тема 6. Основні методології та фреймворки з розробки КЕІ та ІКС.	16	6	-	-	10
Тема 7. Апаратно-програмні платформи створення ІКС.	20	6	-	-	14
Разом за модулем 3	**36**	**12**	**-**	**-**	**24**
Усього годин	**120**	**32**	**16**	**-**	**72**

5. Теми семінарських занять

Не передбачено

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	**2**	**3**
1.	Огляд основних моделей життєвого циклу КЕІ та ІКС	4
2.	Вивчення вимог стандарту ІСО/МЕК 15288-2005. Інформаційна технологія. Системна інженерія. Процеси життєвого циклу систем	4
3.	Огляд основних моделей діагностики кризису в КЕІ (моніторинг зовнішнього середовища КЕІ, аналіз дії конкурентів, аналіз ризиків)	2
4.	Вивчення стандарту ISO 22301 Security and resilience — Business continuity management systems — Requirements	2
5.	Порівняльний аналіз AGILE, SCRUM, RAD, XP	4
	Разом	**16**

7. Теми практичних занять

Не передбачено

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	**Тема 1.** Сучасні практики впровадження системи аудиту інформаційної безпеки на об’єктах КЕІ	24

2.	**Тема 2.** Сучасні методи управління проектами з розробки КЕІ та ІКС (Класичний проектний менеджмент, Lean. Kanban, Six Sigma, PRINCE2)	24
3.	**Тема 3.** Сучасна концепція менеджменту якістю створення КЕІ. Вивчення підходу TQM (Total Quality Management) - всезагальне управління якістю.	24
	Разом	**72**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота здобувачів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, підсумковий контроль у вигляді екзамену.

12. Критерії оцінювання та розподіл балів, які отримують здобувачи

12.1. Розподіл балів, які отримують здобувачи (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	7	0…7
Виконання і захист лабораторних (практичних) робіт	4..7	2	8..14
Модульний контроль	12…14	1	12…14
Змістовний модуль 2			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних (практичних) робіт	4...7	3	12...21
Модульний контроль	14…16	1	14…16
Змістовний модуль 3			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних (практичних) робіт	4...7	-	-
Модульний контроль	14…16	1	14…16
Усього за семестр			**60…100**

Семестровий контроль (іспит/залік) проводиться у разі відмови здобувача від балів поточного тестування й за наявності допуску до іспиту/заліку. Під час

складання семестрового іспиту/заліку здобувач має можливість отримати максимум 100 балів.

Білет для іспиту/заліку складається з двох теоретичних і одного практичного запитання. За перше та друге запитання здобувач отримує по 30 балів, за практичне – 40 балів.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- знати основні положення “Зеленої книги з захисту критичної інфраструктури”.
- знати основні поняття захисту критичної інформаційної інфраструктури, ризик аналізу.
- знати основні процесно-орієнтовані методи забезпечення кібер безпеки.
- Знати основні методи забезпечення інформаційної безпеки підприємства.

Необхідний обсяг вмінь для одержання позитивної оцінки:

- вміти проводити аналіз аварій (кібер інцидентів) із застосуванням моделей.
- вміти застосовувати програмне забезпечення Cafta & Netica для інтегрування методів оцінювання надійності та безпеки смарт грід (ІКС);
- вміти проводити аналіз деградації систем в смарт грід.

12.3 Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60 - 74). Показати необхідний обсяг знань та вмінь для одержання позитивної оцінки відповідно до п.12.2. Захистити не менше 80% від усіх завдань лабораторних занять. Вміти самостійно визначати основні елементи захисту критичної інформаційної інфраструктури та її ризик аналізу. Вміти аналізувати аварій (кібер інциденти) в смарт грід.

Добре (75 - 89). Твердо знать мінімум знань, виконати не менше 90% завдань лабораторних занять. Вміти визначати основні властивості систем, що забезпечують різіліенс. Вміти формулювати та визначати показники різіліенсу. Застосовувати методи та інструментальні засоби оцінювання кібер безпеки, а також методи оцінювання ризиків та кібер безпеки ІКС. Вміти проектувати бізнес-процеси забезпечення кібер безпеки в компанії.

Відмінно (90 - 100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та вміти їх застосовувати.

.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщено за посиланнями:

https://drive.google.com/drive/folders/1mffLqeXDXxmaJERIwRxRFtl7ul9JF4CS

https://mentor.khai.edu/course/view.php?id=3706

14. Рекомендована література

Базова

1. K. Cronin; N. Marion, 2016, Critical Infrastructure Protection, Risk Management, and Resilience – Taylor and Francis; pp. 528.
2. A. Ganguly, U.Bhatia, S. Flynn, 2018, Critical Infrastructures Resilience: Policy and Engineering Principles, Routledge, pp. 132.
3. Yastrebenetsky, M., Kharchenko, V., 2014, "Nuclear power plant instrumentation and control systems for safety and security", IGI Global, pp. 470.
4. M. Yastrebenetsky, V. Kharchenko (Edits), "*Nuclear Power Plant Instrumentation and Control Systems for Safety and Security*", A volume in the Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series, Hershey, Pennsylvania, United States of America, IGI Global, 2014, 470 p.
5. Huffmire, C. Irvine, T.D. Nguyen, "*Handbook of FPGA Design Security*", Springer, 2010, 177 p.
6. V. Kharchenko, A. Kovalenko, V. Sklyar, O. Siora, "Security Assessment of FPGA-based Safety-Critical Systems: US NRC Requirements Context", Proceedings of the International Conference on Information and Digital Technologies (IDT 2015), Žilina, Slovakia, July 7-9, 2015, pp. 117-123.
7. Momoh, J. A, "Fundamentals of analysis and computation for the Smart Grid," Power and Energy Society General Meeting, 2010 IEEE , vol., no., pp.1-5, 25-29 July 2010.
8. Arnold, G. W, "Challenges and Opportunities in Smart Grid: A Position Article," Proceedings of the IEEE, vol.99, no.6, pp.922-927, June 2011.
9. ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary (IDT).
10. NIST SP800-30 Risk Management Guide for Information Technology Systems Text]. – National Institute of Standards and Technology 2002 – 95 p.
11. Byres, E. J., Franz, M. and Miller, D., "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", International Infrastructure Survivability Workshop (IISW '04), IEEE, Lisbon, Portugal, December 4, 2004.
12. Scambray, J. and McClure, S., "Hacking Exposed Windows 2000: Network Security Secrets and Solutions," McGraw_Hill, 2001.
13. B. Utne, P. Hokstad, G. Kjolle, J. Vatn, I.A. Tendel, D. Bertelsen, H. Fridheim, J. Rustrum, Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS approach.

14. U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Washington, DC, 2013.

15. R. Belohlavek, V. Vychodil, Attribute implications in a fuzzy setting, in: B. Ganter, L. Kwuida (Eds.), Lecture Notes in Artificial Intelligence, vol. 3874, Springer-Verlag, Heidelberg, 2015.

Допоміжна

1. Rinaldi, J.Peerenboom Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies /IEEE Control Systems Magazine, Vol. 21 - Dec. 2001 - pp. 11-25.

2. Singer, D. 1990. A fuzzy set approach to fault tree and reliability analysis. FuzzySets and Systems, 34, 2: 145-55.

3. Wayne C. Turner, Steve Doty Energy management handbook, Sixth edition, Fairmont Press, Inc, 2006, 389 p.

4. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1991. Fuzzy variables as a basis for a theory of fuzzy reliability in the possibility context. Fuzzy Sets and Systems, 42, 2: 145-172.

5. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1991. Posbist reliability behavior of typical systems with two types of failures. Fuzzy Sets and Systems, 43, 1:17-32.

6. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1993. Fuzzy states as a basis for a theory of fuzzy reliability. Microelectronic Reliability, 33, 1: 2253-2263.

7. MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects, and Criticality Analysis, 24 Nov. 1980.

8. Pederson, P., Dudenhoeffer, D., Hartley, S. & Perman, M. 2006. Critical Infrastructre Interdependency modelling: A survey of U.S and international research. Report prepared by the Idaho National Laboratory.

15. Інформаційні ресурси

1. The MathWorks. Fuzzy Logic Toolbox. [Ел. ресурс]. URL: http://www.mathworks.com/products/fuzzylogic/

2. NIST Cybersecurity Framework [Ел. ресурс]. URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework.

3. NISTIR 7628 Guidelines for Smart Grid Cyber Security. [Ел. ресурс]. URL: www.nist.gov/smartgrid/upload/nistir-7628.

4. McQueen, M. Quantitative Cyber Risk Reduction Estimation Methodology For A Small SCADA Control System / M. McQueen, Boyer W., Flynn M., Beitel G. [Ел. ресурс]. URL: http://www.inl.gov/technicalpublications/Documents/3303778.