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_____ 2023 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи і технології кібербезпеки
(назва навчальної дисципліни)

Галузь знань: 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво»
(шифр і найменування галузі знань)

Спеціальність: _____
(шифр і назва галузі знань)

Освітня програма: _____
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2023 рік

Робоча програма «Методи і технології кібербезпеки»
(назва навчальної дисципліни)

Розробник: 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 2023 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 – 5.0</td><td rowspan="11">Галузь знань:
10 «Природничі науки»,
11 «Математика та статистика»,
12 «Інформаційні технології»,
15 «Автоматизація та приладобудування»,
16 «Хімічна та біоінженерія»,
17 «Електроніка та телекомунікації»,
19 «Архітектура та будівництво»
(шифр і найменування галузі знань)

Рівень вищої освіти:
другий (магістерський)</td><td>Вибіркова</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>2023/2024</td></tr>
<tr><td>Загальна кількість годин – 64/150</td><td rowspan="2">Семестр: 2
(магістри)</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання:
аудиторних – 2

практичні роботи – 2 (через тиждень)</td></tr>
<tr><td>Лекції *
32 год.</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>32 год.</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>0 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>86 год.</td></tr>
<tr><td>Вид контролю:</td></tr>
<tr><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *64/86*.

* 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 з оцінювання ризиків і кібербезпеки сучасних КІ та інформаційно-керуючих систем (ІКС), використання інструментальних засобів оцінювання ризиків та кібербезпеки.

Завдання: є вивчення базових понять теорії ризиків та кібербезпеки критичних інфраструктур, а також методів її забезпечення.

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

1. **Загальні:**

– здатність до абстрактного мислення, аналізу та синтезу.
– здатність застосовувати знання у практичних ситуаціях.
– здатність планувати та управляти часом.
– навички використання інформаційних і комунікаційних технологій.
– здатність до пошуку, оброблення та аналізу інформації з різних джерел.
– здатність бути критичним і самокритичним.
– здатність генерувати нові ідеї (креативність).
– здатність приймати обґрунтовані рішення.
– здатність працювати автономно.
– здатність розробляти та управляти проектами.
– прихильність безпеці.
– здатність оцінювати та забезпечувати якість виконуваних робіт.
– визначеність і наполегливість щодо поставлених завдань і взятих обов'язків.
– знання іншої мови(мов).

2.Фахові**:**

– здатність до усної та письмової комунікації іноземною мовою.
– базові знання фундаментальних наук в обсязі, необхідному для освоєння загально професійних дисциплін.
– вміння виявляти, аналізувати та вирішувати проблеми у професійній сфері.
– здатність проведення досліджень на відповідному рівні.
– здатність до участі у проектній діяльності; здатність до адаптації та дії в новій ситуації.
– володіння науковими методами обґрунтування, вибору та аналізу криптографічних механізмів і систем захисту.
– готовність використати сучасні досягнення науки і передових технологій.
– здатність розуміти і аналізувати напрями розвитку розподілених систем і мереж, загальної теорії побудови математичних моделей і їх реалізації, теорії і практики керівництва проектами зі створення захищених розподілених інформаційних ресурсів.
– здатність аналізувати системи, моделі та сервіси електронного урядування у секторах «держава – держава», «держава-бізнес», «держава-громадянин» стан надання адміністративних послуг та впроваджувати електроні довірчі послуги у сфері електронного урядування.
– здатність до самостійної науково-дослідної діяльності (аналіз, співставлення, систематизація, абстрагування, моделювання, перевірка достовірності даних, прийняття рішень та ін.), готовність генерувати та використовувати нові ідеї.
– здатність застосовувати професійно-профільовані знання й практичні навички для розв'язання типових задач зі спеціальності.
– здатність самостійної практичної роботи відповідно до отриманої кваліфікації.

Результати навчання: вміти застосовувати методи та інструментальні засоби оцінювання кібербезпеки інформаційно-керуючих систем (ІКС) та критичних інфраструктур (КІ), використовувати методи, що засновані на Байесовських мережах довіри. Мати навички з проектування основних бізнес-процесів із забезпечення кібербезпеки в компанії.

Міждисциплінарні зв'язки: В частині вивчення структур даних дисципліна базується на деяких поняттях дисципліни «Перспективні технології кібербезпеки», а також на поняттях дисципліни «Теорія і технології критичного комп'ютингу».

3. Програма навчальної дисципліни

Модуль 1. Вступ до дисципліни.

Тема 1 Критичні інфраструктури. Основні визначення, класифікація, загрози, вразливості. Основні положення "Зеленої книги з захисту критичної інфраструктури". Смарт грід як нова генерація критичної інформаційної інфраструктури. Основні поняття захисту критичної інформаційної інфраструктури. Основні поняття ризик аналізу.

Тема 2 Ризик менеджмент в контексті кібербезпеки. Локальні та емерджентні ризики. Взаємодія між системами в КІ. Основні моделі кібер інцидентів та атак. Ризик аналіз функціональної безпеки інформаційно-керуючих систем в умовах невизначеності.

Тема 3 Кібер резіліенс КІ та кібер тероризм. . Основні властивості систем, що забезпечують різіліенс. Основні показники оцінювання. Функція відновлення. Кібер тероризм. Методи та інструментальні засоби оцінювання кібербезпеки. Методи оцінювання ризиків та кібербезпеки ІКС.

Практичні завдання.

Семінар. Огляд інструментальних засобів ризик аналізу інформаційної безпеки ІКС та критичної інфраструктури. Практикум. Використання інструментальних засобів для вирішення задач оцінювання кібер ризиків.

Модуль 2. Методи та інструментальні засоби оцінювання кібербезпеки ІКС та КІ.

Тема 4 Нечіткі методи оцінювання кібербезпеки. Поняття нечіткої функції, нечіткої змінної. Функції належності. Нечіткі продукційні системи виводу першого роду. Нечіткі продукційні системи виводу другого роду. Лінгвістичне оцінювання кібербезпеки. Нечітка продукційна система Мамдані-Заде. Нечітка продукційна система Такаги-Сугено-Канга.

Тема 5. Методи оцінювання кібербезпеки та резіліенсу з урахуванням взаємовпливу між системами в КІ. Байесовські мережі довіри та їх застосування для задач оцінювання кібербезпеки. Матричні методи

Модуль 3. Методи та засоби забезпечення кібербезпеки КІ та ІКС.

Тема 6. Основні бізнес-процеси забезпечення кібербезпеки в ІТ компанії. Процесно-орієнтовані методи забезпечення кібербезпеки. Нормативно-правова база України з питань захисту КІ. Аспект кібербезпеки в законодавчій базі України.

Тема 7. Методи забезпечення інформаційної безпеки підприємства. Забезпечення кібербезпеки критичної інфраструктури на прикладі систем критичного застосування (атомна промисловість, банківські системи, тощо). Нормативно-правова база з питань забезпечення кібербезпеки (NIST, IAEA, ISO). Застосування кібер диверсності для забезпечення безпеки КІ.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с.р.
1	2	3	4	5	6
Модуль 1. Вступ до дисципліни					
Тема 1 Критичні інфраструктури.	12	4	10	-	-
Тема 2 Ризик менеджмент в контексті кібербезпеки	18	4	-	-	14
Тема 3 Кібер резіліенс КІ та кібер тероризм	14	4	-	-	10
Разом за модулем 1	**46**	**12**	**10**	**-**	**24**
Модуль 2. Методи та інструментальні засоби оцінювання кібербезпеки ІКС та КІ.					
Тема 4 Нечіткі методи оцінювання кібербезпеки	18	4	8	-	10
Тема 5. Методи оцінювання кібербезпеки та резіліенсу з урахуванням взаємовпливу між системами в КІ.	22	4	8	-	14
Разом за модулем 2	**48**	**8**	**16**	**-**	**24**
Модуль 3. Методи та засоби забезпечення кібербезпеки КІ та ІКС					
Тема 6. Основні бізнес-процеси забезпечення кібербезпеки в ІТ компанії**.**	16	6	6	-	10
Тема 7. Методи забезпечення інформаційної безпеки підприємства.	20	6	-	-	28

1	2	3	4	5	6
Разом за модулем 3	**36**	**12**	**-**	**-**	**24**
Усього годин	**150**	**32**	**32**	**-**	**86**

5. Теми семінарських занять

Не передбачено

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	**2**	**3**
1	Аналіз моделей аварій (кібер інцидентів)	6
2	Огляд та застосування методів аналізу надійності та безпеки смарт грід (ІКС)	6
3	Інтегрування методів оцінювання надійності та безпеки смарт грід (ІКС) із застосуванням прикладного програмного забезпечення (Cafta & Netica)	6
4	Аналіз методів оцінювання деградації систем в смарт грід	6
5	Аналіз деградації систем смарт грід із застосуванням нечітких методів	8
	Разом	**32**

7. Теми практичних занять

Не передбачено

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	**Тема 1.** Огляд методологій з оцінюванняя ризиків кібербезпеки критичних інфрраструктур передових країн світу	24
2	**Тема 2.** Аналіз невизначеності, класифікація типів взаємовпливів між система в КІ.	24
3	**Тема 3.** Вивчення стандарту МЕК 17799:2005 "Інформаційна технологія. Практичні правила керування інформаційної безпекою"	24
	Разом	**72**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

Проведення аудиторних лекцій, лабораторних 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 здобувачі

12.1. Розподіл балів, які отримують здобувачі (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 кібербезпеки.
− 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 кібербезпеки, а також методи оцінювання ризиків та кібербезпеки ІКС. Вміти проектувати бізнес-процеси забезпечення кібербезпеки в компанії.

Відмінно (90 - 100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти 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/u/0/folders/1_as3aHZokjrK7h3hnYFd2wR7MCrANkdi

https://mentor.khai.edu/course/view.php?id=2167

14. Рекомендована література

Базова

1. V. Kharchenko, V. Sklyar, E. Brezhniev, 2013, Safety of information and control systems. Models, techniques and technologies – Palmarium Academic Publishing, pp. 528.
2. R. Bloomfield, K. Netkachova, R. Stroud, 2013, “Security-Informed Safety: If It’s Not Secure, It’s Not Safe”, Software Engineering for Resilient Systems Lecture Notes in Computer Science, Volume 8166, Springer Berlin Heidelberg, pp. 17-32.
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.