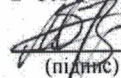


Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Голова НМК


(підпис)

М.С. Зряхов
(ініціали та прізвище)

« 30 » 08 2019 р.

**РОБОЧА ПРОГРАМА ОBOB'ЯЗKОВОЇ
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Методи та технології кібербезпеки критичних інфраструктур
(назва навчальної дисципліни)

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

Спеціальність: 125 Безпека інформаційних і комунікаційних систем
(шифр і назва галузі знань)

Освітня програма: «Комп'ютерні системи та мережі»
(назва освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2019 рік

Робоча програма «Методи та технології кібербезпеки критичних інфраструктур»:
(назва навчальної дисципліни)

для магістрів за спеціальністю: «Безпека інформаційних і комунікаційних систем»,
освітньою програмою «Комп'ютерні системи та мережі»
освітньою програмою «Системне програмування»

« 26 » 08 2019 р., – 11 с.

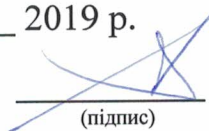
Розробники: Брежнєв Євген Віталійович, професор кафедри 503 д.т.н, с.н.с.
(автор, посада, науковий ступінь та вчене звання)


(підпис)

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

Протокол № 1 від « 30 » 08 2019 р.

Завідувач кафедри д.т.н., професор
(науковий ступінь та вчене звання)


(підпис)

В. С. Харченко
(ініціали та прізвище)

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітня програма, рівень вищої освіти	Характеристика навчальної дисципліни (денна форма навчання)
Кількість кредитів – 4.0	Галузь знань: <u>12</u> <u>«Інформаційні технології»</u> (шифр і найменування галузі знань) Спеціальність: <u>8.125</u> (<u>БІКС</u>) (шифр і назва галузі знань) Освітня програма: <u>«Комп’ютерні системи та мережі»</u> Рівень вищої освіти: освітньо-науковий	Цикл загальної підготовки: Нормативна
Кількість модулів – 3		Навчальний рік
Кількість змістових модулів – не має		2019/2020
Індивідуальне завдання: немає		Семестр: 10 (магістри)
Загальна кількість годин – 48/120		Лекції * <u>32 год.</u>
Кількість тижневих годин для денної форми навчання: аудиторних – 2 лабораторні роботи – 2 (через тиждень)		Практичні, семінарські* <u>0 год.</u>
		Лабораторні * <u>16 год.</u>
		Самостійна робота <u>72 год.</u>
		Вид контролю: іспит

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

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

Результати навчання: вміти застосовувати методи та інструментальні засоби оцінювання кібер безпеки 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 кібер безпеки 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.

Змістовний модуль 1. Вступ до дисципліни.

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

Тема 2 Ризик менеджмент в контексті кібер безпеки. 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 резілієнс КІ та кібер тероризм. . Основні властивості систем, що забезпечують резілієнс. Основні показники оцінювання. Функція відновлення. Кібер тероризм. Методи та інструментальні засоби оцінювання кібер безпеки. Методи оцінювання ризиків та кібер безпеки 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.

Змістовний модуль 2. Методи та інструментальні засоби оцінювання кібер безпеки ІКС та КІ.

Тема 4 Нечіткі методи оцінювання кібер безпеки. Поняття нечіткої функції, нечіткої змінної. Функції належності. Нечіткі продукційні системи виводу першого роду. Нечіткі продукційні системи виводу другого роду. Лінгвістичне оцінювання кібер безпеки. Нечітка продукційна система Мамдані-Заде. Нечітка продукційна система Такаґи-Сугено-Канґа.

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

Змістовний модуль 3. Методи та засоби забезпечення кібер безпеки КІ та ІКС.

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

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

Модульний контроль

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.					
Змістовний модуль 1. Вступ до дисципліни					
Тема 1 Критичні інфраструктури.	12	4	-	8	-
Тема 2 Ризик менеджмент в контексті кібер безпеки	18	4	-	-	14
Тема 3 Кібер резілієнс КІ та кібер тероризм	14	4	-	-	10
Разом за змістовним модулем 1	44	12	-	8	24
Змістовний модуль 2. Методи та інструментальні засоби оцінювання кібер безпеки ІКС та КІ.					
Тема 4 Нечіткі методи оцінювання кібер безпеки	18	4	-	4	10
Тема 5. Методи оцінювання кібер безпеки та резілієнсу з урахуванням взаємовпливу між системами в КІ.	22	4	-	4	14
Разом за змістовним модулем 2	40	8	-	8	24
Змістовний модуль 3. Методи та засоби забезпечення кібер безпеки КІ та ІКС					
Тема 6. Основні бізнес-процеси	16	6	-	-	10

1	2	3	4	5	6
забезпечення кібер безпеки в ІТ компанії.					
Тема 7. Методи забезпечення інформаційної безпеки підприємства.	20	6	-	-	14
Разом за змістовним модулем 3	36	12	-	-	24
Усього годин	120	32	-	16	72

5. Теми семінарських занять

Не передбачено навчальним планом

6. Теми практичних занять

Не передбачено навчальним планом

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	2	3
1	Аналіз моделей аварій (кібер інцидентів)	4
2	Огляд та застосування методів аналізу надійності та безпеки смарт грид (ІКС)	4
3	Інтегрування методів оцінювання надійності та безпеки смарт грид (ІКС) із застосуванням прикладного програмного забезпечення (Cafta & Netica)	2
4	Аналіз методів оцінювання деградації систем в смарт грид	2
5	Аналіз деградації систем смарт грид із застосуванням нечітких методів	4
	Разом	16

8. Самостійна робота

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

9. Індивідуальні завдання

Не передбачено навчальним планом

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, підсумковий контроль у вигляді екзамену.

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (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 студента від балів поточного тестування й за наявності допуску до іспиту/заліку. Під час складання семестрового іспиту/заліку студент має можливість отримати максимум 100 балів.

Білет для іспиту/заліку складається з двох теоретичних і одного практичного запитання. За перше та друге запитання студент 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 грид (ІКС)
- вміти проводити аналіз деградації систем в смарт грид.

12.3 Критерії оцінювання роботи студента 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 грид.

Добре (75 - 89). Твердо знати мінімум знань, виконати не менше 90% завдань лабораторних занять. Вміти визначати основні властивості систем, що забезпечують різілієнс. Вміти формулювати та визначати показники різілієнсу. 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 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

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. Fuzzy Sets 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. Possibilist 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., Dudenhofer, D., Hartley, S. & Perman, M. 2006. Critical Infrastructure Interdependency modelling: A survey of U.S and international research. Report prepared by the Idaho National Laboratory.

15. Інформаційні ресурси

1. The MathWorks. [online]. Fuzzy Logic Toolbox. Available: <http://www.mathworks.com/products/fuzzylogic/> [Dec 16, 2005]
2. [Електронний ресурс]: режим доступа <https://www.cyberriskanalytics.com/>
3. [Електронний ресурс]: режим доступа: <https://www.riskwatch.com/>
4. [Електронний ресурс]: режим доступа: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html
5. [Електронний ресурс]: режим доступа: <http://www.security-risk-analysis.com/introcob.htm>
6. [Електронний ресурс]: режим доступа: <http://www.amenaza.com/index.php>
7. Надеждин, Ю. В. Безопасность АСУ ТП критически важных объектов [Електронний ресурс] / Ю.В. Надеждин – Режим доступа: <http://www.uipdp.com/articles/2014-04/06.html>

8. NIST Cybersecurity Framework [Электронный ресурс] – режим доступа: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework>.
9. NISTIR 7628 Guidelines for Smart Grid Cyber Security[Электронный ресурс] – режим доступа: www.nist.gov/smartgrid/upload/nistir-7628.
10. Воронцов, А.Л. Автоматизированные системы управления технологическими процессами. Вопросы безопасности [Электронный ресурс]/А.Л. Воронцов –Режим доступа: <http://www.jetinfo.ru/stati/informatsionnaya-bezopasnost-promyshlennykh-obektov>.
11. Юдин, А.А. Анализ и оценка нормативных документов, применяемых для обеспечения информационной безопасности SMART GRID систем [Электронный ресурс] / А.А. Юдин, Г. В. Пирогов – Режим доступа: pnzzi.kpi.ua/25/25_p88.pdf.
12. McQueen, M. Quantitative Cyber Risk Reduction Estimation Methodology For A Small SCADA Control System [Электронный ресурс] / М. McQueen, Boyer W., Flynn M., Beitel G. – Режим доступа: <http://www.inl.gov/technicalpublications/Documents/3303778>.