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

Технології зеленої ІТ-інженерії
(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:_____
(код та найменування спеціальності)

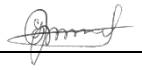
Освітня програма: _____
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

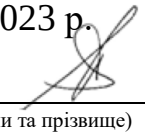
Харків 2023 рік

Робоча програма «Технології зеленої ІТ-інженерії»:
(назва навчальної дисципліни)

Розробники: Брежнєв Євген Віталійович, професор 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="14">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)

Рівень вищої освіти:
другий (магістерський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td rowspan="2">Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 4</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: 1</td></tr>
<tr><td rowspan="10">Кількість тижневих годин для денної форми навчання:
аудиторних – 2

лабораторні роботи – 4 (через тиждень)</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td>32 год.</td></tr>
<tr><td>Практичні, семінарські *</td></tr>
<tr><td>0 год.</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>32 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>86 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: *64/86*

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

2. Мета та завдання навчальної дисципліни

Мета вивчення: отримання здобувачами теоретичних знань і навичок з оцінювання ризиків і безпеки при проектуванні інтелектуальних КЕІ, використання інструментальних засобів моделювання параметрів їх систем.

Завдання: вивчення методології та практиці оцінювання, забезпечення безпеки інтелектуальних енергетичних інфраструктур як нового покоління енергоефективних та енергозберігаючих систем, спрямованих на вирішення існуючих екологічних проблем.

Здобувачі 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.

Програмні результати навчання: вміти застосовувати методи оцінювання та забезпечення безпеки критичних енергетичних інфраструктур та

енергоефективних систем. Застосовувати бездротові системи управління в задачах електроенергетики.

Міждисциплінарні зв'язки: В частині вивчення структур даних дисципліна базується на деяких поняттях дисципліни «Інженерія програмного забезпечення». В частині вивчення концепцій та технологій обробки та зберігання великих даних дисципліна є підґрунтям для дисципліни «Технології обробки великих даних».

3. Програма навчальної дисципліни

Модуль 1
Змістовний модуль 1. Методи і інструментальні засоби моделювання КЕІ

Тема 1. Вступ до теорії інтелектуальних енергоінфраструктур - нового покоління зелених КЕІ. Smart Grid. Визначення, технології, принципи та завдання. Огляд основних IT в смарт грід. Smart Metering, SCADA/EMS (SCADA/DMS), Demand Response, Embedded generation control; WAMS; Dynamic Line Ratings. Стан впровадження технологій в передових країнах світу.

Тема 2. Моделі та основні атрибути смарт грід. Основні підходи до моделювання КЕІ. Невизначеності. Аналіз підходів до моделювання інтелектуальних енергоінфраструктур.

Тема 3. Огляд основних методологій ризик аналізу КЕІ.
Better Infrastructure Risk and Resilience (BIRR). Protection of Critical Infrastructures – Baseline Protection Concept. Carver 2. Critical Infrastructure Modelling Simulation (CIMS). Critical Infrastructure Protection Decision Support System. Critical Infrastructure Protection modelling and Analysis. Sandia Risk Assessment Methodology. Аналіз і оцінка ризиків в інтелектуальних енергоінфраструктурах.

Змістовний модуль 2. Нечіткі методи та інформаційні технології аналізу функціональної безпеки в КЕІ

Тема 4. Основні положення технології Soft-computing (SC). Нечітке керування складними процесами. Застосування нечітких методів оцінювання безпеки ядерного реактору. Функції належності. Лінгвістичні змінні.
Тема 5. Огляд методів аналізу безпеки інтелектуальних КЕІ. Огляд нечітких методів аналізу безпеки інтелектуальних КЕІ.
Тема 6. Огляд інструментальних засобів нечіткого аналізу безпеки інтелектуальних КЕІ.

Змістовний модуль 3. Методи і інформаційні технології оцінювання кібербезпеки КЕІ

Тема 6. Огляд і аналіз поточних проблем оцінювання інформаційної безпеки (ІБ) в КЕІ. Основні виклики безпеки. Ризики ІБ. Стан інформаційної безпеки. Основні етапи аналізу ризиків в КЕІ.

Тема 7. Огляд основних методів аналізу ІБ в КЕІ. Огляд інструментальних засобів оцінювання ІБ в КЕІ. RiskWatch. COBRA. Buddy System. Застосування ІЗ Netica для аналізу кібер безпечних систем в КЕІ.

Змістовний модуль 4. Бездротові технології в сучасних засобах автоматизації зелених ІТ інфраструктур

Тема 8. Основні характеристики бездротових технологій. Класифікація бездротових мереж. Етапи розвитку технологій. Технічні характеристики. Основні переваги і недоліки.

Тема 9. Застосування бездротової системи управління в задачах електроенергетики. Досвід застосування бездротових технологій в енергетиці. Загальна характеристика явища пробою. Життєвий цикл розробки на прикладі системи контролю стану діелектриків.

Тема 10. Застосування бездротової системи управління в задачах управління освітленням. Загальна концепція розумного будинку. Підходи до реалізації управління освітленням. Недоліки і переваги. Основні підходи до розробки систем бездротового освітлення.

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. Методи і інструментальні засоби моделювання КЕІ					
Тема 1. Вступ до теорії інтелектуальних енергоінфраструктур - нового покоління зелених КЕІ.	14	4	-	-	5
Тема 2. Моделі та основні атрибути смарт грід (безпека, надійність, тощо)	16	2	-	4	5
Тема 3. Огляд основних ІЗ моделювання КЕІ.	18	4	-	4	5
Разом за змістовний модулем 1	**48**	**10**	**-**	**8**	**15**
Змістовний модуль 2. Нечіткі методи та інформаційні технології аналізу функціональної безпеки в КЕІ					
Тема 4. Основні положення технології Soft-computing (SC).	14	4	-	-	10
Тема 5. Огляд методів аналізу безпеки інтелектуальних КЕІ**.**	18	4	-	4	10
Тема 6. Огляд інструментальних засобів нечіткого аналізу безпеки інтелектуальних КЕІ.	16	2		4	10
Разом за змістовний модулем 2	**48**	**10**	**-**	**8**	**30**
Змістовний модуль 3. Методи і інформаційні технології оцінювання кібербезпеки КЕІ					
Тема 6. Огляд і аналіз поточних проблем оцінювання інформаційної безпеки (ІБ) в КЕІ.	12	2	-	-	8
Тема 7. Огляд основних методів аналізу ІБ в КЕІ.	28	4	-	4	7
Разом за змістовний модулем 3	**40**	**6**	**-**	**4**	**15**
Змістовний модуль 4. Бездротові технології в сучасних засобах автоматизації зелених ІТ інфраструктур					
Тема 8. Основні характеристики бездротових технологій	16	2	-	4	14
Тема 9. Застосування бездротової системи управління в задачах електроенергетики**.**	6	2		4	
Тема 10. Застосування бездротової системи управління в задачах управління освітленням.	18	2		4	12
Разом за змістовний модулем 4	**44**	**6**	**-**	**12**	**26**
Усього годин	**150**	**32**	**-**	**32**	86

5. Теми семінарських занять

Не передбачено

6. Теми практичних занять

Не передбачено

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	**2**	3
1	Огляд і застосування методів ризик аналізу інтелектуальних енергетичних інфраструктур.	2
2	Ознайомлення з ІЗ імітаційного моделювання інтелектуальних КЕІ. Вивчення пакету моделювання GridLabD.	2
3	Застосування методів аналізу надійності та безпеки смарт грід	1
4	Дослідження параметрів розподільних мереж КЕІ з використанням пакета Energy Storage.	1
5	Дослідження параметрів розподільних мереж ІЕІ з використанням пакету Voltage Control.	1
6	Дослідження параметрів розподільних мереж ІЕІ з використанням пакету Solar	1
7	Аналіз безпеки КЕІ з використанням пакета Fuzzy Logic Toolbox.	1
8	Застосування інструментальних засобів для оцінювання ІБ в КЕІ.	1
9	Ознайомлення з платою SmartRF06 и CC2538, операційною систмеою OSAL, його API, HAL.	2
10	Вивчення збіру даних з вбудованій периферії плати SmartRF06 по таймеру.	4
11	Вивчення вбудованої периферії плати розширення SmartRF06, можливостей операційної системи OSAL для роботи з периферії.	4
12	Налаштування мережі на основі ZigBee за схемою «точка-точка» із застосуванням плати – розширення SmartRF06.	4
13	Налаштування мережі на основі Zig-Bee за схемою «точка-множина точок» на основі SmartRF06.	4
14	Налаштування мережі на основі ZigBee із застосуванням с маршрутизації даних, із використанням плати-розширення SmartRF06.	4
	Разом	**32**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	**Тема 1**. Проектування цифрових підстанцій. Аспекти реалізації вимог до програмного та апаратного забезпечення і	10
2	**Тема 2.** Перспективи реалізації зеленої енергетики в Україні	10
3	**Тема 3.** Вивчення досвіду реалізації програм впровадження технології смарт грід передових країн Європи	10
4	**Тема 4.** Дослідження бездротових систем керування типу “розумний будинок”	16
5	**Тема 5.** Вивчення перспектив створення малих модульних реакторів (ММР) як альтернативного зеленого джерела електричної енергії. Огляд основних проектів ММР	20
6	**Тема 6.** Огляд перспективних інформаційних технологій в проектах ММР	20
	Разом	**86**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота здобувачів за відповідними матеріалами (п.10,11).

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

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	0,5…1	4	2…4
Виконання і захист лабораторних (практичних) робіт	2...4	5	10..20
Модульний контроль	8…10	1	8…10

Змістовний модуль 2			
Робота на лекціях	0…1	4	0…4
Виконання і захист лабораторних (практичних) робіт	2...4	1	2...4
Модульний контроль	3…5	1	3…5
Змістовний модуль 3			
Робота на лекціях	0,5 …1	4	2…4
Виконання і захист лабораторних (практичних) робіт	2...4	1	2...4
Модульний контроль	3…5	1	3…5
Змістовний модуль 4			
Робота на лекціях	0,33…1	3	1…3
Виконання і захист лабораторних (практичних) робіт	3...4	8	24...32
Модульний контроль	3…5	1	3…5
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 види загальні визначення, технології, принципи, основні ІТ в смарт грід;

– знати характеристики методів аналізу та оцінки ризиків в інтелектуальних енергоінфраструктурах;

– знати основні етапи аналізу ризиків в смарт грід;

– знати класифікацію бездротових мереж;

Необхідний обсяг вмінь для одержання позитивної оцінки:

– вміти проводити налаштування мережі на основі ZigBee за схемою «точка-точка» із застосуванням плати – розширення SmartRF06;

– вміти проводити налаштування мережі на основі Zig-Bee за схемою «точка-множина точок» на основі SmartRF06;

– вміти налаштовувати мережі на основі ZigBee із застосуванням с маршрутизації даних, із використанням плати-розширення SmartRF06.

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 давати характеристику основним методам аналізу ризиків та забезпечення безпеки зелених інфраструктур, знати нечіткі методи та інформаційні технології аналізу функціональної безпеки в КЕІ. Вміти проводити імітаційне моделювання інтелектуальних КЕІ за допомогою GridLabD.
Добре (75 - 89). Твердо знать мінімум знань, виконати не менше 90% завдань лабораторних занять. Знати методи і інформаційні технології оцінювання кібербезпеки КЕІ, знати загальні підходи щодо застосування бездротової системи управління в задачах електроенергетики, а також в задачах управління освітленням. Вміти проводити аналіз безпеки КЕІ з використанням пакета Fuzzy Ligic Toolbox, вміло застосовувати інструментальні засоби для оцінювання ІБ в КЕІ. Вміти проводити налаштування плати SmartRF06 и CC2538, операційну систему OSAL.

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 посиланням: https://mentor.khai.edu/course/view.php?id=5308

14. Рекомендована література

Базова

1. Зеленая ИТ-инженерия. В двух томах. Том 1. Принципы, модели, компоненты / Под ред. Харченко В.С. – Х.: Нац. аэрокосмический ун-т им. Н.Е.Жуковского «ХАИ», 2014. – 594 с.
2. NPP I&C Systems for Safety and Security. M. Yastrebenetsky, V. Kharchenko (editors). USA, IGI-Global, 2014.
3. Zadeh L. and Kacprzyk J. Computing with Words in Information/Intelligent Systems – Part 1: Foundation; Part 2: Applications. Heidelberg, Germany: Physica-Verlag, vol.1, 187 – 201, 1991.
4. Li Chen, et al. Modelling and Simulation of Power Grid Engineering Project based on System Dynamics on the Background of Smart Grid. Systems Engineering Procedia Volume 3, 2012 - P. 92–99

5. Peng H.L., Huang H.H., Hsiao C.T., Han K.C., Lin C.T.System dynamics approach to the financial crisis in elementary education system-a case in Taiwan, in proceedings of ICMIT 2010, Singapore, 2010.
6. E. Alishahi, M. Parsa Moghaddam, M.K. Sheikh-El-Eslami. A system dynamics approach for investigating impacts of incentive mechanisms on wind power investment. Renewable Energy, 2011 – P. 310-317.
7. A.S. White. A control system project development model derived from System Dynamics, International Journal of Project Management, 2011 – P. 696-705.
8. P. Crucitti, et al. Model for cascading failures in complex networks, Physical Review E, vol. 69, 2004.

Допоміжна

1. J. Lin, et al., A General Framework for Quantitative Modeling of Dependability in Cyber-Physical Systems: A Proposal for Doctoral Research. Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, pp. 668-671, 2009.
2. J. Nutaro, "Designing power system simulators for the smart grid: combining controls, communications, and electro-mechanical dynamics," Proceedings of the 2011 IEEE Power Engineering Society General Meeting, 2011.
3. C. P. Nguyen and A. J. Flueck, "Modeling of communication latency in smart grid," Proceedings of the 2011 IEEE Power and Energy Society General Meeting, 2010.
4. Kremers, E., et al. A complex systems modelling approach for decentralized simulation of electrical microgrids. In 15th IEEE International Conference on Engineering of Complex Computer Systems, 2010, page 8, Oxford.
5. 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
6. U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. Washington, DC, 2013.
7. ZT Taylor, K Gowri et al. GridLAB-D Technical Support Document: Residential End-Use Module Version 1.0/ Prepared for the U.S. Department of Energy under Contract DE-AC05-76RL018302008 – 30 P.
8. R. Belohlavek, V. Vychodil, Attribute implications in a fuzzy setting, in: B. Ganter, L. Kwuida (Eds.), ICFCA 2006, Lecture Notes in Artificial Intelligence, vol. 3874, Springer-Verlag, Heidelberg, 2015.
9. V. Novak, Mathematical fuzzy logic in modeling of natural language semantics, in: P. Wang, D. Ruan, E. Kerre (Eds.), Fuzzy Logic – A Spectrum of Theoretical & Practical Issues, Elsevier, Berlin, 2015.
10. W. Pedrycz, F. Gomide, Fuzzy Systems Engineering: Toward Human-Centric Computing, Wiley-IEEE Press, 2015.
11. I. Perfilieva, Fuzzy transforms: a challenge to conventional transforms, in: P.W. Hawkes (Ed.), Advances in Images and Electron Physics, vol. 147, Elsevier Academic Press, San Diego, 2015.

12. Uziel Sandler, Lev Tsitolovsky Neural Cell Behavior and Fuzzy Logic. Springer, 2015.
13. Ganga, D.M., Carpinetti, L. (2011) "A fuzzy logic approach to supply chain performance management". Int. J. Production Economics 134, 2015.
14. Sirigiri, P., & Gangadhar, P.V., & Kajal, K.G. Evaluation of teacher's performance using Fuzzy Logic Techniques. International Journal of Computer Trends and Technology, 2012.
15. Nomesh, B., Pranav, S., & Jalaj, B. Quantification of agility of a Supply Chain using Fuzzy Logic. American Journal of Engineering and Applied Sciences: 2 (2), 2012.
16. Mehrdad, M., & Abbas N. A. Supplier Performance Evaluation Based On Fuzzy Logic. International Journal of Applied Science and Technology, 1(5), 2011.
17. NIST SP800-30 Risk Management Guide for Information Technology Systems [Text]. – National Institute of Standards and Technology Special Publication 800-30 Natl. Inst. Stand. Technol. Spec. Publ. 800-30, 2002 - 54 pages
18. Marcel Frigault and Lingyu Wang. Measuring network security using bayesian network-based attack graphs. [Text] In STPSA'09, 2009.
19. Marcel Frigault, Lingyu Wang, Anoop Singhal, and Sushil Jajodia. Measuring network security using dynamic bayesian network. [Text] In Proceedings of the 4th ACM workshop on Quality of protection, 2009.
20. Finn V. Jensen, "Bayesian Networks and Decision Graphs" [Text], Springer-Verlag 2001.
21. Daniel Burroughs, Linda Wilson, and George Cybenko. "Analysis of Distributed Systems Using Bayesian Methods." [Text] Performance, Computing, and Communications Conference, 2002. 21st IEEE International , 2002 Page(s): 329 –334
22. D. Heckerman, "Bayesian Networks for Data Mining,"[Text] Data Mining and Knowledge Discovery, 1997.
23. P. Cheeseman and J. Stutz, 1996. Bayesian classification (Auto Class): theory and results in Advances in Knowledge Discovery and Data Mining, edited by U.M. Fayyad et al., California: The AAAI Press, pp: 61-83
24. Risk management: a tool for improving Nuclear Power Plant performance, IAEA VIENNA, IAEA-TECDOC-1209, 2001.
25. NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses, Idaho National Laboratory Idaho Falls, Idaho 83415, 2010.
26. Common Cybersecurity Vulnerabilities in Industrial Control Systems, Home Land Security, Control Systems Security program, National Cyber security Division, 2011.
27. Max Wandera, Brent Jonasson, Cybersecurity considerations for electrical distribution systems. White Paper WP152002EN, 2014.
28. Common vulnerabilities in critical infrastructure control systems, Sandia National Laboratories Albuquerque, NM 87185-0785, 2nd edition, 2003.

15. Інформаційні ресурси

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