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

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
_____ В. В. Павліков
(підпис) (ініціали та прізвище)
«31» 08 2020 р.
Відділ аспірантури і докторантури

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і методи зеленої ІТ-інженерії
(назва навчальної дисципліни)

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

Спеціальність: 125 «Кібербезпека»
(шифр і назва спеціальності)

Освітньо-наукова програма: «Кібербезпека»
(назва освітньої програми)

Рівень вищої освіти: третій (освітньо-науковий)

Форма навчання: денна

Харків 2020 рік

РОБОЧА ПРОГРАМА
ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і методи зеленої ІТ-інженерії
(назва дисципліни)

для здобувачів за спеціальністю 125 "Кібербезпека"

освітньо-наукової програми Кібербезпека

«26» серпня 2020 р., – 14 с.

Розробник: професор, д.т.н., с.н.с. _____ Брежнєв Є.В.
(посада, науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

Гарант ОНП доцент, к.т.н., доцент _____ Колісник М.О.
(посада, науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

Протокол №1 від «27» серпня 2020 р. засідання кафедри № 503

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

ПОГОДЖЕНО:

Завідувач відділу
аспірантури і докторантури _____ В. Б. Селевко

Голова наукового товариства
студентів, аспірантів,
докторантів і молодих вчених _____ Т. П. Старовойт

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітня програма, рівень вищої освіти	Характеристика навчальної дисципліни *Денна форма навчання*
Кількість кредитів – 7.0	**Галузь знань** 12 «Інформаційні технології» (шифр і найменування)	Вибіркова з переліку 1 Вибіркові компоненти з глибинних знань зі спеціальності
Кількість модулів – 1		**Навчальний рік**
Кількість змістовних модулів – 4	**Спеціальність** 125 «Кібербезпека» (код і найменування)	2020/2021
Індивідуальне завдання: немає		**Семестр**
Загальна кількість годин – 80/210	**Освітньо-наукова програма** «Кібербезпека» (найменування)	1-й
Кількість тижневих годин для денної форми навчання: аудиторних – **5**, самостійної роботи аспіранта – **8**	**Рівень вищої освіти**: третій (освітньо-науковий)	**Лекції** * 48 год. **Практичні, семінарські** * 32 год. **Лабораторні*** 0 год. **Самостійна робота** 130 год. **Вид контролю**: іспит

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *80/130*

[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 аспірантами теоретичних знань і навичок з оцінювання ризиків і безпеки при проектуванні інтелектуальних КЕІ, використання інструментальних засобів моделювання параметрів їх систем в наукових дослідженнях.

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

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

загальні:

- здатність до абстрактного мислення, аналізу та синтезу;
- здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- здатність працювати в міжнародному контексті,

спеціальні (фахові):

- здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у кібербезпеці та дотичних до неї (нього, них) міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та суміжних галузей;
- здатність усно і письмово презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок українською та англійською мовами, глибоке розуміння англомовних наукових текстів за напрямом досліджень;
- здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності;
- здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері кібербезпеки;
- здатність дотримуватись етики досліджень, а також правил академічної доброчесності в наукових дослідженнях та науково-педагогічній діяльності;
- системний науковий світогляд та загальнокультурний кругозір;
- здатність до продукування нових ідей і розв'язання комплексних проблем у галузі інформаційних технологій, а також до застосування сучасних методологій, методів та інструментів педагогічної та наукової діяльності в кібербезпеці;
- здатність моделювати, аналізувати функціональну безпеку, оцінювати КЕІ у різних предметних галузях, у тому числі аерокосмічній галузі.

Програмні результати навчання

Мати передові концептуальні та методологічні знання з кібербезпеки і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.

Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки державною та

іноземною мовами, кваліфіковано відображати результати досліджень у наукових публікаціях у провідних міжнародних наукових виданнях.

Формулювати і перевіряти гіпотези, використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень (опитувань, спостережень та інше) і математичного та/або комп'ютерного моделювання, наявні літературні дані.

Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.

Глибоко розуміти загальні принципи та методи кібербезпеки, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері кібербезпеки та у викладацькій практиці.

Здійснювати пошук та критичний аналіз інформації, концептуалізацію та реалізацію наукових проектів з кібербезпеки.

Знати сучасні підходи та засоби моделювання досліджуваних об'єктів та процесів управління, в тому числі в аерокосмічній галузі, вміти створювати нові, вдосконалювати та розвивати методи математичного і комп'ютерного моделювання складних систем, оптимізації та прийняття рішень.

Знати, розуміти та вміти застосовувати методи та засоби створення інформаційних технологій та програмного забезпечення розподілених систем, Інтернету речей, хмарних обчислень, систем штучного інтелекту, віртуальної реальності у різних предметних областях, в тому числі в аерокосмічній галузі.

Знати філософсько-світоглядні засади, сучасні тенденції, напрямки і закономірності розвитку вітчизняної та світової науки в умовах глобалізації й уміння їх використовувати в науково-дослідній та професійній діяльності у різних предметних галузях, у тому числі аерокосмічній галузі.

Знати, розуміти та вміти застосовувати методи та інструментальні засоби моделювання, аналізу функціональної безпеки, оцінювання КЕІ в аерокосмічній галузі.

Міждисциплінарні зв'язки: Дисципліна є вибірковою компонентою освітньо-наукової програми «Кібербезпека» і базується на знаннях, отриманих під час вивчення дисципліни «Обробка та аналіз результатів наукових досліджень з використанням ІТ», що є обов'язкової компонентою.

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін вибіркової компоненти переліку 2.

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 ІТ 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 7. Огляд і аналіз поточних проблем оцінювання інформаційної безпеки (ІБ) в КЕІ для наукових досліджень. Основні виклики безпеки. Ризики ІБ. Стан інформаційної безпеки. Основні етапи аналізу ризиків в КЕІ.

Тема 8. Огляд основних методів аналізу ІБ в КЕІ в наукових дослідженнях. 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 9 Основні характеристики бездротових технологій. Класифікація бездротових мереж. Етапи розвитку технологій. Технічні характеристики. Основні переваги і недоліки.

Тема 10 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 11 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 змістовних 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	-	-	10
Тема 2. Моделі та основні атрибути смарт грід (безпека, надійність, тощо)	22	6	4	-	12
Тема 3. Огляд основних ИС моделювання КЕІ. Модульний контроль	18	4	4	-	10
Разом за змістовний модулем 1	**54**	**14**	**8**	**-**	**32**
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.	22	8	4	-	10
Тема 6. Огляд інструментальних засобів нечіткого аналізу безпеки інтелектуальних КЕІ. Модульний контроль	16	2	4	-	10
Разом за змістовний модулем 2	**52**	**14**	**8**	**-**	**30**
Змістовний модуль 3. Методи і інформаційні технології оцінювання кібербезпеки КЕІ					
Тема 7. Огляд і аналіз поточних проблем оцінювання інформаційної безпеки (ІБ) в КЕІ для наукових досліджень.	26	6	-	-	20
Тема 8. Огляд основних методів аналізу ІБ в КЕІ в наукових дослідженнях. Модульний контроль	20	4	4	-	12
Разом за змістовний модулем 3	**46**	**10**	**4**	**-**	**32**
Змістовний модуль 4. Бездротові технології в сучасних засобах автоматизації зелених ІТ інфраструктур					
Тема 9. Основні характеристики бездротових технологій	20	2	4	-	14
Тема 10. Застосування бездротової системи управління в задачах електроенергетики.	20	6	4	-	10
Тема 11. Застосування бездротової системи управління в задачах управління освітленням. Модульний контроль	18	2	4	-	12
Разом за змістовний модулем 4	**58**	**10**	12	**-**	**36**
Усього годин	**210**	**48**	**32**	**-**	130

5. Теми семінарських занять

Не передбачено навчальним планом

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	**Тема 1.** Проектування цифрових підстанцій. Аспекти реалізації вимог до програмного та апаратного забезпечення	30
2	**Тема 2.** Перспективи реалізації зеленої енергетики в Україні	20
3	**Тема 3.** Вивчення досвіду реалізації програм впровадження технології смарт грід передових країн Європи	20
4	**Тема 4.** Дослідження бездротових систем керування типу "розумний будинок"	10
5	**Тема 5.** Вивчення перспектив створення малих модульних реакторів (ММР) як альтернативного зеленого джерела електричної енергії. Огляд основних проектів ММР	30
6	**Тема 6.** Огляд перспективних інформаційних технологій в проектах ММР	20
	Разом	**130**

9. Індивідуальні завдання

Не передбачено навчальним планом

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота аспірантів за відповідними матеріалами.

11. Методи контролю

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

12. Критерії оцінювання та розподіл балів, які отримують аспіранти

12.1. Розподіл балів, які отримують аспіранти (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 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 практичних робіт	2...4	1	2...4
Модульний контроль	3…5	1	3…5
Змістовний модуль 3			

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	**2**	3
1	Огляд і застосування методів ризик аналізу інтелектуальних енергетичних інфраструктур.	2
2	Ознайомлення з ІС імітаційного моделювання інтелектуальних КЕІ. Вивчення пакету моделювання GridLabD.	2
3	Застосування методів аналізу надійності та безпеки смарт грид	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**

7. Теми лабораторних занять

Не передбачено навчальним планом

Робота на лекціях	0,5 …1	4	2…4
Виконання і захист 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 практичних робіт	3...4	8	24...32
Модульний контроль	3…5	1	3…5
Усього за семестр			**60 - 100**

Семестровий контроль (іспит) проводиться у разі відмови аспіранта від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту аспірант має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних і одного практичного запитання. За перше та друге запитання аспірант 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 аспіранта 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 практичних робіт. 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 практичних робіт. 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 Logic Toolbox, вміло застосовувати інструментальні засоби для оцінювання ІБ в

KEI. 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://drive.google.com/drive/u/0/folders/1hFYHK_881-_b0pZL5muNjom_W1phDGuh

14. Рекомендована література

Базова

1. Зелена IT-інженерія. У двох томах. Том 1. Принципи, моделі, компоненти / Под ред. Харченко В.С. - Х .: Нац. аерокосмічний ун-т ім. М. Є. Жуковського «ХАІ», 2014. - 594 с.
2. Надєждін, Ю. В. Безпека АСУ ТП критично важливих об'єктів [Електронний ресурс] / Ю.В. Надєждін - Режим доступу: http://www.uipdp.com/articles/2014-04/06.html, 2014.
3. Ніцель, Л. В. 6 кроків до інформаційної безпеки АСУ ТП [Електронний ресурс] / Л. В. Ніцель - Режим доступу: http://ua.automation.com/content/6-shagov-k-informacionnoj-bezopasnosti-asu-tp, 2014.
4. Гарбук, Н.В Стандартизація в області забезпечення інформаційної безпеки АСУ ТП [Електронний ресурс] /Н.В. Гарбук - Режим доступу: http://www.slideshare.net/phdays/ss-8360192 -2014.
5. Лукацький, А.В. Безпека АСУ ТП: від слів до справи [Електронний ресурс] / А.В. Лукацький Режим доступу: http://www.slideshare.net/lukatsky/ss-14279925 - 2014.
6. Воронцов, А. Л. Автоматизовані системи управління технологічними процесами. Питання безпеки [Електронний ресурс] /А.Л Воронцов - Режим доступу: http://www.jetinfo.ru/stati/informatsionnaya-bezopasnost-promyshlennykh-obektov/2011/?nid=77f3dbdaa8dfb77077c0888a712a3e1a-2014.
7. Юдін, А.А. Аналіз і оцінка нормативних документів, що застосовуються для забезпечення інформаційної безпеки SMART GRID систем [Електронний

ресурс] / А.А. Юдін, Г.В. Пірогов- Режим доступу: pnzzi.kpi.ua/25/25_p88.pdf - 2014.

8. Варфоломєєв, А.А. Управління інформаційними ризиками [Текст]: Навч. посібник. / А.А. Варфоломєєв - М .: РУДН, 2008. - 158 с.

9. NPP I&C Systems for Safety and Security. M. Yastrebenetsky, V. Kharchenko (editors). USA, IGI-Global, 2014.

10. 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.

Допоміжна

1. 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

2. 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.

3. 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.

4. A.S. White. A control system project development model derived from System Dynamics, International Journal of Project Management, 2011 – P. 696-705.

5. P. Crucitti, et al. Model for cascading failures in complex networks, Physical Review E, vol. 69, 2004.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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

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

12. 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.

13. 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.

14. 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.

15. W. Pedrycz, F. Gomide, Fuzzy Systems Engineering: Toward Human-Centric Computing, Wiley-IEEE Press, 2015.

16. 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.

17. Uziel Sandler, Lev Tsitolovsky Neural Cell Behavior and Fuzzy Logic. Springer, 2015.

18. Ganga, D.M., Carpinetti, L. (2011) "A fuzzy logic approach to supply chain performance management". Int. J. Production Economics 134, 2015.

19. 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.

20. 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.

21. Mehrdad, M., & Abbas N. A. Supplier Performance Evaluation Based On Fuzzy Logic. International Journal of Applied Science and Technology, 1(5), 2011.

22. 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

23. Marcel Frigault and Lingyu Wang. Measuring network security using bayesian network-based attack graphs. [Text] In STPSA'09, 2009.

24. 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.

25. Finn V. Jensen, "Bayesian Networks and Decision Graphs" [Text], Springer-Verlag 2001.

26. 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

27. D. Heckerman, "Bayesian Networks for Data Mining,"[Text] Data Mining and Knowledge Discovery, 1997.

28. 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

29. Risk management: a tool for improving Nuclear Power Plant performance, IAEA VIENNA, IAEA-TECDOC-1209, 2001.

30. NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses, Idaho National Laboratory Idaho Falls, Idaho 83415, 2010.

31. Common Cybersecurity Vulnerabilities in Industrial Control Systems, Home Land Security, Control Systems Security program, National Cyber security Division, 2011.

32. Max Wandera, Brent Jonasson, Cybersecurity considerations for electrical distribution systems. White Paper WP152002EN, 2014.

15. Інформаційні ресурси

1. Керівництво користувача Netica [Електронний ресурс]: режим доступу www.norsys.com
2. Хабрахабр [Електронний ресурс]: режим доступу http://habrahabr.ru/company/surfingbird/blog/176461/
3. [Електронний ресурс]: режим доступу http://www.habarov.spb.ru/new_es/exp_sys/es06/es6.htm
4. Студопедія [Електронний ресурс]: режим доступу http://studopedia.org/7-129207.html
5. http://www.dis.anl.gov/projects/ri.html
6. http://www.bmi.bund.de
7. http://www.ni2cie.org/CARVER2.asp
8. The MathWorks. [online]. Fuzzy Logic Toolbox. Available: http://www.mathworks.com/products/fuzzylogic/ [Dec 16, 2005]