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 » серпня 2021 р.

СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і методи 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

Спеціальність: 101 Екологія, 103 Науки про Землю, 113 Прикладна математика, 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки, 123 Комп'ютерна інженерія, 124 Системний аналіз, 125 Кібербезпека, 151 Автоматизація та комп'ютерно-інтегровані технології, 152 Метрологія та інформаційно-вимірювальна техніка, 163 Біомедична інженерія, 172 Телекомунікації та радіотехніка, 173 Авіоніка, 193 Геодезія та землеустрій

Освітня програма: усі освітні програми за відповідними спеціальностями

Рівень вищої освіти: ***другий (магістерський)***

Силабус введено в дію з 01.09.2021 року

Харків – 2021 р.

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

Силабус навчальної дисципліни розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки (№ 503)

Протокол № 1 від « 30 » серпня 2021 р.

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

Погоджено з представником здобувачів освіти:

_____ _____ _____
(підпис) (ініціали та прізвище)

1. Загальна інформація про викладача

Брежнєв Євген Віталійович, д.т.н., професор. З 2017 з року викладає в університеті наступні дисципліни:
Теорія і методи зеленої ІТ-інженерії;
Методи та технології створення критичних ІТ-інфраструктур;
Методи та технології кібербезпеки критичних інфраструктур.
Напрями наукових досліджень: Функціональна та кібербезпека інформаційно-керуючих систем та критичних інфраструктур, Забезпечення якості програмних засобів, Моделювання бізнес процесів, Цифрова трансформація ІТ індустрії.

2. Опис навчальної дисципліни

Семестр, в якому викладається дисципліна – 1 семестр.

Обсяг дисципліни:

5 кредитів ЄКТС (150 годин), у тому числі аудиторних – 64 годин, самостійної роботи здобувачів – 86 годин.

Форми здобуття освіти

Денна, дистанційна, дуальна.

Дисципліна – вибіркова.

Види навчальної діяльності – лекції, лабораторні роботи, самостійна робота здобувача.

Види контролю – поточний, модульний та підсумковий (семестровий) контроль (іспит).

Мова викладання – українська.

Необхідні обов'язкові попередні дисципліни (пререквізити) – Інженерія програмного забезпечення.

Необхідні обов'язкові супутні дисципліни (кореквізити) – Технології розроблення та забезпечення функціональної безпеки ІУС; Технології забезпечення кібербезпеки апаратних та програмованих засобів.

3. Мета та завдання навчальної дисципліни

Мета

Отримання студентами (аспірантами) 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.

Після опанування дисципліни здобувач набуде наступні **компетентності:**

Здатність аналізувати дані та оцінювати необхідні знання для розв'язання задач підвищення надійності, функціональної безпеки та кібербезпеки, живучості комп'ютерних систем та цифрових сервісів з використанням сучасних математичних методів, зокрема штучного інтелекту, комп'ютерного моделювання тощо.

Здатність комунікувати іноземними мовами з представниками різних галузей знань та сфер діяльності з метою з'ясування їх потреб при створенні комп'ютерних систем.

Здатність інтегрувати знання з різних дисциплін, застосовувати системний підхід та враховувати нетехнічні аспекти при розв'язанні інженерних задач та проведенні досліджень.

Здатність аргументувати вибір методу розв'язання наукової задачі, критично оцінювати отримані результати та захищати прийняті рішення.

Очікується, що після опанування дисципліни здобувач будуть досягнуті наступні **результати навчання** і він буде:

– Вміти проводити пошук інформації в спеціалізований літературі, використовуючи різноманітні ресурси: журнали, бази даних, on-line ресурси.

– Вміти використовувати набуті знання за допомогою аналітичного апарату і логічного мислення, уміти застосовувати їх у наукових дослідженнях.

– Вміти застосовувати міри ризику, оцінювати та використовувати їх у наукових дослідженнях.

– Вміти використовувати здобуті у наукових дослідженнях навички, необхідні для ефективної педагогічної та викладацької діяльності.

– Вміти використовувати набуті навички для організації діяльності і спілкування з керівництвом та колегами.

4. Зміст навчальної дисципліни

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 критичних 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.

Модульний контроль.

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.

Модульний контроль.

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.

Модульний контроль.

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.

5. Індивідуальні завдання

Не передбачено навчальним планом

6. Методи навчання

Словесні, наочні, практичні.

7. Методи контролю

Поточний контроль (теоретичне опитування й розв'язання практичних завдань), модульний контроль (тестування за розділами курсу) та підсумковий (семестровий) контроль (іспит).

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

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**

Контроль знань при проведенні занять оцінюється за такими шкалами:

1) активність на лекції під час відповідей на питання:

– повна відповідь на питання – 2 бали;

– неповна відповідь – 1 бал;

– відсутність на лекції – 0 балів;

2) виконання і захист лабораторних робіт:

– виконані всі завдання лабораторної роботи, оформлені відповідно до вимог, надано вичерпні правильні відповіді на всі запитання – 4 бали;

– виконані всі завдання лабораторної роботи, мають місце незначні відхилення від оформлення відповідно до вимог, надано правильні відповіді на всі запитання – 3 бали;

– виконано 75-99% завдань лабораторної роботи, мають місце незначні відхилення від оформлення відповідно до вимог, надано правильні відповіді не на всі запитання – 2 бали;

– виконано 50-74% завдань лабораторної роботи, мають місце значні відхилення від оформлення відповідно до вимог, надано правильні відповіді не на всі запитання – 1 бал;

– студент не допущений до захисту роботи (виконано менше 50% її завдань) або робота не захищена – 0 балів.

На модульний контроль (всього 18 балів) виносяться всі пройдені за контрольований період теми, які включаються у варіанти тестових завдань, що містять по 18 питань. Максимальна кількість балів за кожне питання – 1.

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до заліку. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

Прийнята шкала оцінювання

Сума балів за всі види навчальної діяльності	Оцінка для екзамену, *курсового проекту* (роботи), практики
90-100	відмінно
75-89	добре
60-74	задовільно
01-59	незадовільно з можливістю повторного складання

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60 - 74). Показати необхідний обсяг знань та вмінь для одержання позитивної оцінки, а саме:

– 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.

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.

9. Політика навчального курсу

Відпрацювання пропущених занять відбувається відповідно до розкладу консультацій, за попереднім погодженням з викладачем. Питання, що стосуються академічної доброчесності, розглядає викладач або за процедурою, визначеною у Положенні про академічну доброчесність.

10. Методичне забезпечення та інформаційні ресурси

Навчально-методичний комплекс дисципліни розміщено за посиланням:

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

1. Руководство пользователя Netica [Электронный ресурс]: режим доступа www.norsys.com
2. Хабрахабр [Электронный ресурс]: режим доступа http://habrahabr.ru/company/surfingbird/blog/176461/
3. [Электронный ресурс]: режим доступа http://www.habarov.spb.ru/new_es/exp_sys/es06/es6.htm
4. Студопедия [Электронный ресурс]: режим доступа 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]

11. 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. Надеждин, Ю. В. Безопасность АСУ ТП критически важных объектов [Электронный ресурс] / Ю.В. Надеждин – Режим доступа: http://www.uipdp.com/articles/2014-04/06.html, 2014.
3. Ницель, Л. В. 6 шагов к информационной безопасности АСУ ТП [Электронный ресурс] /Л. В. Ницель – Режим доступа: http://ua.automation.com/content/6-shagov-k-informacionnoj-bezopasnosti-asu-tp, 2014.
4. Гарбук, Н.В Стандартизация в области обеспечения информационной безопасности АСУ ТП [Электронный ресурс] /Н.В. Гарбук – Режим доступа: http://www.slideshare.net/phdays/ss-8360192 –2014.
5. Лукацкий, А.В. Безопасность АСУ ТП: от слов к делу [Электронный ресурс] / А.В. Лукацкий Режим доступа: http://www.slideshare.net/lukatsky/ss-14279925 – 2014.
6. 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/2011/?nid=77f3dbdaa8dfb77077c0888a712a3e1a–2014.
7. 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 –2014.

8. Варфоломеев, А.А. Управление информационными рисками [Текст]: Учеб. пособие./ А.А. Варфоломеев – 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.

33. Common vulnerabilities in critical infrastructure control systems, Sandia National Laboratories Albuquerque, NM 87185-0785, 2nd edition, 2003.