Силабус освітнього компонента
Програма навчальної дисципліни

Системний інжиніринг

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
8

Мова викладання
Українська

Викладачі, розробники

Мілевський Станіслав Валерійович
stanislav.milevskyi@khpi.edu.ua
кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Науковий Гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій» у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна програма дисципліни "Системний інжиніринг" визначає зміст і обсяг знань, необхідних для фахівця в галузі розробки та впровадження комплексних інженерних систем. Дисципліна охоплює проблематику розробки, аналізу та управління життєвим циклом складних систем, починаючи від концептуального проектування і до їх експлуатації та утилізації. Особливу увагу приділяється використанню сучасних інструментів моделювання, аналізу і оптимізації інженерних систем. Лабораторні заняття допомагають студентам закріпити отримані знання на практиці.

Мета та цілі дисципліни

Метою вивчення дисципліни є формування у майбутніх фахівців знань та вмінь, необхідних для проектування, розробки та впровадження складних технічних систем з урахуванням вимог надійності, безпеки та ефективності.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.

ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 24 год., лабораторні роботи – 12 год., самостійна робота – 54 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Основи математичного моделювання систем безпеки

Особливості дисципліни, методи та технології навчання

Викладання дисципліни передбачає використання пояснювально-ілюстративного та репродуктивного методів, а також активізацію навчально-пізнавальної діяльності через презентації, індивідуальні та групові проекти, моделювання систем, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ до системного інжинірингу.
Основні поняття та визначення. Життєвий цикл систем. Вимоги до систем.
Тема 2. Процеси системного інжинірингу.
Моделі життєвого циклу. Управління вимогами. Аналіз та оцінка альтернатив.
Тема 3. Системний підхід до проектування.
Концептуальне проектування. Синтез та аналіз рішень. Моделювання систем.
Тема 4. Оцінка продуктивності та надійності систем.
Основи надійності. Аналіз ризиків. Оцінка експлуатаційних характеристик систем.
Тема 5. Моделювання та симуляція в системному інжинірингу.
Методи моделювання. Інструменти для симуляції. Прикладні задачі моделювання.
Тема 6. Управління проектами системного інжинірингу.
Планування та організація проекту. Контроль виконання та управління ризиками.
Тема 7. Інтеграція систем.
Підходи до інтеграції. Випробування та верифікація систем. Вимоги до сумісності.
Тема 8. Життєвий цикл систем.
Підтримка, модернізація та утилізація систем. Економічний аналіз та оцінка вартості життєвого циклу.
Тема 9. Управління конфігурацією.
Контроль версій. Управління змінами. Підтримка конфігурації.
Тема 10. Сучасні тренди у системному інжинірингу.
Глобальні тенденції в автоматизації, кіберфізичні системи, штучний інтелект у системному інжинірингу.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Основи моделювання систем.
Тема 2. Розробка концептуальної моделі системи.
Тема 3. Моделювання та симуляція динамічних систем.
Тема 4. Оцінка надійності системи.

Тема 5. Аналіз ризиків у проекті.
Тема 6. Інтеграція підсистем у комплексні системи.
Тема 7. Управління вимогами до системи.
Тема 8. Використання інструментів для управління конфігурацією.
Тема 9. Управління проектами з використанням спеціалізованих інструментів.
Тема 10. Верифікація та валідація систем.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Blanchard, Benjamin S. Systems Engineering and Analysis. Pearson Education, 2013. https://books.google.com.ua/books/about/Systems_Engineering_and_Analysis.html?id=tC-pBwAAQBAJ&redir_esc=y
2. Sage, Andrew P., and James E. Armstrong. Introduction to Systems Engineering. Wiley, 2000. https://books.google.com.ua/books/about/Introduction_to_Systems_Engineering.html?id=of4VEAAAQBAJ&redir_esc=y
3. Stevens, Richard, Peter Brook, Ken Jackson, and Stuart Arnold. Systems Engineering: Coping with Complexity. Pearson Education, 1998. https://www.scenarioplus.org.uk/reviews/stevens.htm

Додаткова література

4. INCOSE. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. Wiley, 2015. https://download.e-bookshelf.de/download/0003/6422/62/L-G-0003642262-0007580512.pdf
5. Maier, Mark W., and Eberhardt Rechtin. The Art of Systems Architecting. CRC Press, 2009. http://ndl.ethernet.edu.et/bitstream/123456789/38076/1/43.pdf
6. Wasson, Charles S. System Engineering Analysis, Design, and Development: Concepts, Principles, and Practices. Wiley, 2015. https://lib.manaraa.com/books/System%20Analysis%20Design%20%201209577.pdf

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•іспит: 40% семестрової оцінки

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено

28.08.2024 — Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП
Роман КОРОЛЬОВ