



Силабус освітнього компонента

Програма навчальної дисципліни



Системний інжиніринг

Шифр та назва спеціальності

К4 – Управління інформаційною безпекою

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Спеціалізація**Кафедра**

Кібербезпеки (328)

Освітня програма

Управління інформаційною безпекою

Тип дисципліни

Вибіркова

Рівень освіти

Перший (бакалаврський)

Форма навчання

Денна

Семестр

8

Мова викладання

Українська

Викладачі, розробники

**МІЛЕВСЬКИЙ Станіслав Валерійович**

stanislav.milevskyi@khpi.edu.ua

Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» 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 заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.

СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.

СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.

СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.

СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.

СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.

СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. 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.

РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.

РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.

РН11. 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.

РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.

РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.

PH17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.

PH18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

PH19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-комунікаційних системах.

PH20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.

PH21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.

PH22. 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 – 10 год., лабораторні роботи – 20 год., самостійна робота – 60 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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до системного інжинірингу. Процеси системного інжинірингу. Основні поняття та визначення. Життєвий цикл систем. Вимоги до систем. Моделі життєвого циклу. Управління вимогами. Аналіз та оцінка альтернатив.	2
Тема 2. Системний підхід до проектування. Оцінка продуктивності та надійності систем. Концептуальне проектування. Синтез та аналіз рішень. Моделювання систем. Основи надійності. Аналіз ризиків. Оцінка експлуатаційних характеристик систем.	2
Тема 3. Моделювання та симуляція в системному інжинірингу. Управління проектами системного інжинірингу. Методи моделювання. Інструменти для симуляції. Прикладні задачі моделювання. Планування та організація проекту. Контроль виконання та управління ризиками.	2
Тема 4. Інтеграція систем. Життєвий цикл систем. Управління конфігурацією. Підходи до інтеграції. Випробування та верифікація систем. Вимоги до сумісності. Підтримка, модернізація та утилізація систем. Економічний аналіз та оцінка	2

вартості життєвого циклу. Контроль версій. Управління змінами. Підтримка конфігурації.

Тема 5. Сучасні тренди у системному інжинірингу.

2

Глобальні тенденції в автоматизації, кіберфізичні системи, штучний інтелект у системному інжинірингу.

Загальна кількість годин

10

Лабораторні заняття

Теми лабораторних занять

Кількість
годин

Вагові
коефіцієнти a

Тема 1. Основи моделювання систем.

2

0,2

Ознайомлення з базовими принципами моделювання, типами моделей та їх застосуванням для аналізу систем.

Тема 2. Розробка концептуальної моделі системи.

2

0,2

Побудова концептуальної моделі, визначення структури та ключових елементів системи.

Тема 3. Моделювання та симуляція динамічних систем.

2

0,2

Створення моделей динамічних процесів та їх симуляція для оцінки поведінки системи у різних умовах.

Тема 4. Оцінка надійності системи.

2

0,2

Методи аналізу надійності, прогнозування відмов та розрахунок експлуатаційних характеристик.

Тема 5. Аналіз ризиків у проєкті.

2

0,2

Ідентифікація та оцінка ризиків, методи управління ризиками та мінімізація впливу на проєкт.

Тема 6. Інтеграція підсистем у комплексні системи.

2

0,2

Об'єднання підсистем, забезпечення сумісності, перевірка взаємодії та функціонування інтегрованої системи.

Тема 7. Управління вимогами до системи.

2

0,2

Методи збору, класифікації та контролю вимог, управління змінами у вимогах.

Тема 8. Використання інструментів для управління конфігурацією.

2

0,2

Застосування сучасних інструментів для контролю версій, відстеження змін та підтримки конфігурації системи.

Тема 9. Управління проєктами з використанням спеціалізованих інструментів.

2

0,2

Планування, контроль виконання та управління ресурсами проєкту за допомогою спеціалізованого програмного забезпечення.

Тема 10. Верифікація та валідація систем.

2

0,2

Перевірка відповідності системи технічним вимогам та оцінка її придатності до експлуатації.

Загальна кількість годин

20

$\sum_{i=1}^n a_i = 2$

Контрольні роботи

Теми контрольних робіт

Вагові
коефіцієнти b

Тема 1. Моделювання, оцінка та управління складними системами.

0,2

Перевірка знань та умінь студентів з побудови концептуальних та динамічних моделей систем, оцінки надійності та ризиків, інтеграції підсистем, управління вимогами та конфігурацією, а також застосування методів верифікації та валідації систем.

Загалом

$\sum_{i=1}^m b_i = 0,2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення

Кількість годин

Тема 1. Методи оптимізації складних систем.

8

Дослідження підходів до оптимізації продуктивності та ресурсів у складних системах.

Тема 2. Кіберфізичні системи та IoT у системному інжинірингу.

8

Особливості проектування та управління інтегрованими фізичними та цифровими системами.

Тема 3. Аналіз та моделювання ризиків у критичних системах.

8

Методи оцінки ризиків, побудова сценаріїв і моделювання наслідків.

Тема 4. Системна інтеграція та інтероперабельність.

9

Стратегії інтеграції підсистем та забезпечення сумісності різномірних компонентів.

Тема 5. Системний підхід до життєвого циклу програмних продуктів.

9

Планування, підтримка, модернізація та утилізація ПЗ з урахуванням системних принципів.

Тема 6. Моделювання і симуляція поведінки користувачів у системах.

9

Використання агентного та дискретного моделювання для оцінки реакцій користувачів.

Тема 7. Сучасні тренди в автоматизації та цифрових двійниках.

9

Дослідження технологій цифрових двійників, автоматизації та вплив штучного інтелекту на системне проектування.

Загальна кількість годин

60

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.

Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

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

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k :

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,4	0,2		0,4

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.

Розрахунок підсумкової оцінки проводиться за формулою:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \Pi_k \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль

I – оцінка за виконання індивідуального завдання

K – середньозважена оцінка за контрольні роботи

Π_k – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \dots + K_m \cdot b_m}{\sum_{i=1}^m b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, К, І, ...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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

Здобувач вищої освіти 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

30.08.2025



Завідувач кафедри

Сергій ЄВСЄЄВ

30.08.2025



Гарант ОП

Роман КОРОЛЬОВ