



## Силабус освітнього компонента

Програма навчальної дисципліни



# Системний інжиніринг

**Шифр та назва спеціальності**

F5 – Кібербезпека та захист інформації

**Інститут**

ННІ комп'ютерних наук та інформаційних технологій

**Спеціалізація****Кафедра**

Кібербезпеки (328)

**Освітня програма**

Кібербезпека

**Тип дисципліни**

Вибіркова

**Рівень освіти**

Перший (бакалаврський)

**Форма навчання**

Денна, заочна

**Семестр**

8

**Мова викладання**

Українська, англійська

---

## Викладачі, розробники

**МІЛЕВСЬКИЙ Станіслав Валерійович**

[stanislav.milevskyi@khpi.edu.ua](mailto: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

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та систем захисту інформації.

СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

## Результати навчання

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.

PH14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації.

PH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

PH16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

PH17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

PH20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

PH21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

## Обсяг дисципліни

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

### Навчальні заняття

#### Лекції

| Теми лекцій                                                                                                                                                                                                                                              | Кількість годин |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Тема 1. Вступ до системного інжинірингу. Процеси системного інжинірингу.</b><br>Основні поняття та визначення. Життєвий цикл систем. Вимоги до систем. Моделі життєвого циклу. Управління вимогами. Аналіз та оцінка альтернатив.                     | 2               |
| <b>Тема 2. Системний підхід до проектування. Оцінка продуктивності та надійності систем.</b><br>Концептуальне проектування. Синтез та аналіз рішень. Моделювання систем. Основи надійності. Аналіз ризиків. Оцінка експлуатаційних характеристик систем. | 2               |
| <b>Тема 3. Моделювання та симуляція в системному інжинірингу. Управління проектами системного інжинірингу.</b><br>Методи моделювання. Інструменти для симуляції. Прикладні задачі моделювання. Планування та організація проекту. Контроль виконання та  | 2               |

управління ризиками.

**Тема 4. Інтеграція систем.**

2

Підходи до інтеграції. Випробування та верифікація систем. Вимоги до сумісності.

**Тема 5. Життєвий цикл систем. Управління конфігурацією.**

2

Підтримка, модернізація та утилізація систем. Економічний аналіз та оцінка вартості життєвого циклу. Контроль версій. Управління змінами. Підтримка конфігурації.

**Тема 6. Сучасні тренди у системному інжинірингу.**

2

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

**Загальна кількість годин**

**12**

**Лабораторні заняття**

Теми лабораторних занять

Кількість  
годин

Вагові  
коефіцієнти  $\alpha$

**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 проекті.**

2

0,2

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

**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 проектами з використанням спеціалізованих інструментів.**

4

0,2

Планування, контроль виконання та управління ресурсами проекту за допомогою спеціалізованого програмного

забезпечення.

**Тема 10. Верифікація та валідація систем.**

4

0,2

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

**Загальна кількість годин**

**24**

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

**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 матеріалу**

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.**

8

Стратегії інтеграції підсистем та забезпечення сумісності різномірних компонентів.

**Тема 5. Системний підхід до життєвого циклу програмних продуктів.**

8

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

**Тема 6. Моделювання і симуляція поведінки користувачів у системах.**

7

Використання агентного та дискретного моделювання для оцінки реакцій користувачів.

**Тема 7. Сучасні тренди в автоматизації та цифрових двійниках.**

7

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

**Загальна кількість годин**

**54**

## 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](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](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<br>(практичні, семінарські,<br>лабораторні заняття), $k_1$ | Контрольні роботи<br>(за наявності), $k_2$ | Індивідуальне<br>завдання<br>(за наявності), $k_3$ | Підсумковий контроль<br>(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:

$$O = П \cdot k_1 + K \cdot k_2 + I \cdot k_3 + Пк \cdot k_4$$

де:  $\Pi$  – середньозважена середня оцінка за поточний контроль  
 $I$  – оцінка за виконання індивідуального завдання  
 $K$  – середньозважена оцінка за контрольні роботи  
 $\Pi_k$  – 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 ( $\Pi$ ,  $K$ ,  $I$ ,...) 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  $O$  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<br>(потрібне додаткове вивчення) | FX   |
| 1–34       | Незадовільно<br>(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 ЄВСЕЄВ

30.08.2025



**Гарант ОП**  
Сергій ЄВСЕЄВ