**Силабус освітнього компонента**
Програма навчальної дисципліни

# Моделювання кіберфізичних дій

**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**
Професійна підготовка, Вибіркова

**Рівень освіти**
Другий (магістерський)

**Форма навчання**
Денна, заочна

**Семестр**
2

**Мова викладання**
Українська, англійська

## Викладачі, розробники

**ПОГАСІЙ Сергій Сергійович**
Serhii.Pohasii@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Гарант освітньо-науової програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.

Детальніше про викладача на сайті кафедри

# Загальна інформація

## Анотація

Навчальна дисципліна "Моделювання кіберфізичних дій" є вибірковою навчальною дисципліною. Дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця з кібербезпеки та дозволяють вирішувати професійні задачі, що базуються на організації та моделюванні дій в кризових ситуаціях пов'язаних з кібербезпекою.

## Мета та цілі дисципліни

Підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також фахівців з моделювання кіберфізичних дій, на базі освоєння принципів та методів збору цифрової інформації для дослідження поведінки агентів систем безпеки, проведення статичного аналізу індивідуальної та групової поведінки учасників кіберфізичних дій, використовуючи інструменти та методи різноманітних напрямків кібербезпеки.

## Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

## Компетентності

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

## Результати навчання

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

### Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

### Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології, Основи криптографічного захисту, Основи програмування.

### Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

## Програма навчальної дисципліни

### Навчальні заняття

#### Лекції

| Теми лекцій | Кількість годин |
|---|---|
| **Тема 1. Вступ. Моделювання.**<br>Цілі та завдання навчальної дисципліни «Моделювання кіберфізичних дій». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів.<br>Основні поняття моделювання, поняття системи та моделі, основні типи моделей, види моделей та їх класифікація за різними критеріями, вимоги до моделей. | 2 |
| **Тема 2. Основні види моделювання. Формальні методи побудови моделей. Принципи побудови моделей. Технологія моделювання.**<br>Основні види моделювання (аналітичне, імітаційне, статистичне), їх характеристики та відношення між собою. Формальні методи побудови моделей: кібернетичний підхід, системна динаміка, теоретично-множинний підхід.<br>Основні принципи побудови моделей: інформаційної достатності, доцільності, здійсненності, множинності моделей, агрегації, параметризації, застосування методології ітераційного багаторівневого моделювання. Технологія моделювання: основні етапи, їх взаємозв'язок та характеристики. | 2 |
| **Тема 3. Ідентифікація параметрів математичної моделі. Адекватність,** | 2 |

| | |
|---|---|
| **чутливість, непротирічність моделі. Структуровані підходи до збирання інформації.**<br>Постановка завдання ідентифікації, основні етапи його вирішення та їх взаємозв'язок. Поняття адекватності, чутливості та непротирічності моделі, формальні способи їх перевірки.<br>Методи розвідки із відкритим вихідним кодом. Огляд методів структурованого аналізу. Типи інформації, що збирається: ділова інформація (фінансова, клієнти, постачальники, партнери). Інформація про IT-інфраструктуру. Виявлення джерел інформації. | |
| **Тема 4. Основні поняття і визначення, що використовуються при описі моделей безпеки комп'ютерних систем. Соціальна інженерія.**<br>Елементи теорії комп'ютерної безпеки. Сутність, суб'єкт, доступ, інформаційний потік. Класична класифікація загроз безпеки інформації. Види інформаційних потоків. Види політик управління доступом та інформаційними потоками. Витік права доступу і порушення безпеки КС. Математичні основи моделей безпеки.<br>Соціальна інженерія. Огляд проекту «Інструментарій соціальної інженерії». | 2 |
| **Тема 5. Системно-динамічні моделі дій у кіберпросторі. Мова системної динаміки. Побудова імітаційних моделей.**<br>Концепція системної динаміки. Класифікація систем. Методи вивчення складних систем. Системний аналіз та системна динаміка. Понятийний апарат. Основні поняття. Типи зв'язків між елементами системи. Класифікація та позначення елементів моделі.<br>Формування цілей дослідження. Збір інформації про систему та процеси (етап референції). Побудова концептуальної моделі. Побудова машинної моделі. Проведення імітаційних експериментів та верифікація моделі. Обговорення моделі (дебрифінг). Поліпшення моделі. | 2 |
| **Тема 6. Теоретико-ігрові моделі дій у кіберпросторі. Застосівання теорії ігор для моделювання кіберфізичних дій.**<br>Елементи теорії ігор. Ігри та їх класифікація. Чисті стратегії гравців. Змішана стратегія гравців. Матричні ігри. Мінімаксні стратегії. Гра з сідловою точкою. Гра без сідловою точкою. Вирішення матричної гри. Критерії оптимальності стратегії адміністратора. Методи розв'язання матричних ігор. Домінування. Використання лінійного програмування. Біматричні ігри. Рівноваги Неша у кінцевій грі N осіб. Дилема ув'язненого. Програмне забезпечення знаходження рішення ігор. Нескінченні ігри.<br>Приклад матричної гри "зловмисник - адміністратор". Програмне застосування для вибору оптимального набору засобів захисту. Відображення атак у кіберпросторі. Вибір засобу ефективного захисту від DoS/DDoS-атак. Моделювання поведінки азартного зловмисника. | 2 |
| **Тема 7. Агентні моделі кіберфізичних дій.**<br>Об'єкти та агенти. Класифікація агентів кіберфізичних систем. Мультіагентні системи. Взаємодія агентів у кіберпросторі. Комунікація та координація кіберфізичних агентів. Кооперація та конфронтація агентів. Моделі конфліктних ситуацій у кіберпросторі. | 2 |
| **Тема 8. Планування дій у кібер-фізичних системах. Навчання у кіберфізичних системах. Розпізнавання у кібер-фізичних системах.**<br>Планування дій. Планування при синтезі програм. Вчинки та поведінка. Моделі навчання. Навчання за прикладами. Навчальні системи. Проблема розпізнавання. Математична теорія розпізнавання образів. Розпізнавання атак. Розпізнавання зловмисників. Алгоритмічні основи знань. | 2 |
| **Загальна кількість годин** | **16** |

## Лабораторні заняття

## Контрольні роботи

| Теми лабораторних занять / Теми контрольних робіт | Кількість годин | Вагові коефіцієнти $b$ | Вагові коефіцієнти $a$ |
|---|---|---|---|
| **Тема 1. Основи моделювання кіберфізичних дій, види моделей, формальні методи та ідентифікація параметрів.**<br>Ознайомлення з інструментарієм MATLAB для побудови моделей поведінки кіберфізичних систем та проведення базових симуляцій.<br>Охоплює основні поняття моделювання, типи та класифікації моделей, принципи побудови моделей, технологію моделювання, ідентифікацію параметрів математичної моделі, а також методи збору інформації про систему та оцінку адекватності, чутливості та непротирічності моделі. | 6 | | 0,1<br>0,2 |
| **Тема 2. Використання системи SIMULINK для моделювання дій у кіберфізичних системах.**<br>Створення графічних моделей динамічних процесів у середовищі SIMULINK. | 6 | | 0,1 |
| **Тема 3. Системно-динамічне, теоретико-ігрове та агентне моделювання, планування та розпізнавання дій у кіберфізичних системах.**<br>Включає побудову системно-динамічних моделей, використання теорії ігор для моделювання атак та захисту, застосування агентних моделей, координацію агентів у кіберпросторі, планування дій, навчання агентів та алгоритми розпізнавання атак зловмисників. | 4 | | 0,1 |
| **Тема 4. Моделювання кіберфізичних дій мережею Петрі.**<br>Використання мереж Петрі для формалізації взаємодії агентів, опису послідовностей дій та синхронізації процесів у кіберфізичних системах. | 4 | | 0,1 |
| **Тема 5. Основи побудови системно-динамічних моделей за допомогою PowerSim. Побудова імітаційної моделі взаємодії «зловмисник-захисник».**<br>Розробка системно-динамічних моделей для оцінки ефективності заходів захисту та прогнозування поведінки атакуючих і захисних агентів. | 4 | | 0,1 |
| **Тема 6. Побудова та використання ігрової моделі «Відбиття атак у кіберпросторі».**<br>Застосування теорії ігор для моделювання конфліктних ситуацій між атакуючими та захисними агентами, вибір оптимальних стратегій захисту. | 4 | | 0,1 |
| **Тема 7. Мультиагентна модель поведінки та взаємодії агентів у кіберфізичній системі.**<br>Моделювання взаємодії кількох агентів у кіберфізичній системі, координації дій, співпраці та конфронтації, аналіз сценаріїв безпечного функціонування системи. | 4 | | 0,1 |
| **Загальна кількість годин** | **32** | **Загалом**<br>Побудова кінцевих автоматів для опису поведінки окремих агентів у кіберпросторі та аналіз їхніх станів і переходів.<br>$\sum_{i=1}^{m} b_i = 0{,}2$ | $\sum_{i=1}^{n} a_i = 0{,}8$ |

## Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

## Опрацювання теоретичного матеріалу

| Теми для самостійного вивчення | Кількість годин |
|---|---|

| | |
|---|---|
| **Тема 1 Методи формального моделювання кіберфізичних систем.** Вивчення кібернетичного, теоретико-множинного та системного підходів до формалізації моделей кіберфізичних дій. | 8 |
| **Тема 2. Принципи ітераційного та багаторівневого моделювання.** Дослідження підходів до побудови моделей на кількох рівнях абстракції та застосування ітераційного підходу для уточнення моделі. | 8 |
| **Тема 3. Методи оцінки адекватності та чутливості моделей.** Аналіз способів перевірки точності моделей, виявлення впливу змін параметрів на поведінку системи. | 7 |
| **Тема 4. Соціальна інженерія та її моделювання.** Дослідження атак соціальної інженерії, методів їх прогнозування та включення у моделі кіберфізичних дій. | 7 |
| **Тема 5. Імітаційне моделювання кіберфізичних атак.** Побудова імітаційних моделей для відтворення сценаріїв DoS/DDoS, шкідливого ПЗ та інших атак. | 7 |
| **Тема 6. Теорія ігор у кібербезпеці.** Вивчення стратегій атакуючих і захисників, матричних ігор, мінімаксних стратегій, рівноваги Неша та їх застосування у кіберфізичних системах. | 7 |
| **Тема 7. Агентні підходи до моделювання кіберфізичних систем.** Розгляд типів агентів, їхньої взаємодії, координації та протидії загрозам у мультиагентних системах. | 7 |
| **Тема 8. Планування дій у кіберфізичних системах.** Методи автоматизованого планування дій агентів, синтез програмних сценаріїв та моделювання поведінки у критичних ситуаціях. | 7 |
| **Тема 9. Навчання та адаптація агентів у кіберпросторі.** Вивчення методів машинного навчання та адаптивних стратегій для агентів кіберфізичних систем. | 7 |
| **Тема 10. Розпізнавання атак та аномалій у кіберфізичних системах.** Застосування математичної теорії розпізнавання образів та алгоритмів детекції аномалій для виявлення зловмисників і атак у реальному часі. | 7 |
| **Загальна кількість годин** | **72** |

## 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. Томашевський В.М, Моделювання систем. – К. Видавнича група BHV, 2005. – 352 с. [Електронний ресурс]. – Режим доступу:

https://pdf.lib.vntu.edu.ua/books/2016/Tomashev_2005_352.pdf
2. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020. – 241 с. [Електронний ресурс]. – Режим доступу: http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf
3. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с. [Електронний ресурс]. – Режим доступу: https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover
4. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0. [Електронний ресурс]. – Режим доступу: https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf.

### Додаткова література

5. Жерновий Ю. В. Імітаційне моделювання систем масового обслуговування: Практикум. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2007. – 307 с. [Електронний ресурс]. – Режим доступу: https://new.mmf.lnu.edu.ua/wp-content/uploads/2018/02/Imit_model.pdf
6. Shoham, Yoav, and Kevin Leyton-Brown, «Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations». Cambridge University Press, 2009. [Електронний ресурс]. – Режим доступу: https://www.masfoundations.org/mas.pdf
7. Sun, Ron, Cognition and Multi-Agent Interaction: From Cognitive Modeling to Social Simulation. Cambridge University Press,2006. [Електронний ресурс]. – Режим доступу: http://www.cambridge.org/uk/catalogue/catalogue.asp?isbn=0521839645.
8. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. [Електронний ресурс]. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O.Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. [Електронний ресурс]. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. [Електронний ресурс]. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

## 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), $k_4$ |
|---|---|---|---|
| 0,8 | 0,2 | | |

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:

$$О = П \cdot k_1 + К \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
$K$ – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

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

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

де: $b_i$ - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, $K$, 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**<br>Сергій ЄВСЕЄВ |
| | 30.08.2025 |  | **Гарант ОП**<br>Ольга КОРОЛЬ |