**Силабус освітнього компонента**
Програма навчальної дисципліни

# Системно-динамічне моделювання кіберконфліктів

**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

**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 "Системно-динамічне моделювання кіберконфліктів" охоплює сучасні підходи до моделювання та аналізу кіберконфліктів з використанням методів системної динаміки. Студенти отримають знання щодо моделювання динамічних процесів у сфері кібербезпеки, розробки сценаріїв кіберконфліктів, а також аналізу взаємодії кіберзагроз та заходів захисту. Лабораторні заняття спрямовані на закріплення практичних навичок побудови моделей, що дозволить студентам опанувати інструменти моделювання реальних кіберконфліктів.

## Мета та цілі дисципліни

Метою дисципліни є формування знань та навичок щодо моделювання кіберконфліктів із використанням підходів системної динаміки для аналізу кіберзагроз та розробки ефективних стратегій кіберзахисту.

## Формат занять

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

## Компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
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.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно 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

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
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.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
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.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики 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.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки 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)

Основи кібербезпеки, Технології програмування, Основи математичного моделювання систем безпеки.

### 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 до системної динаміки та моделювання кіберконфліктів.** Основи системної динаміки. Типові кіберконфлікти. Застосування системної динаміки у кібербезпеці. | 2 |
| **Тема 2. Кіберзагрози та їх динаміка.** Види кіберзагроз. Моделювання кіберзагроз та їх впливу на системи. | 2 |

| | |
|---|---|
| **Тема 3. Моделювання захисних механізмів у кіберпросторі.** Оцінка ефективності заходів кіберзахисту. Побудова моделей протидії кіберзагрозам. | 2 |
| **Тема 4. Сценарії кіберконфліктів.** Аналіз типових сценаріїв кіберконфліктів. Моделювання динамічної ескалації кіберконфліктів. | 2 |
| **Тема 5. Системні петлі зворотного зв'язку у кіберконфліктах.** Аналіз позитивних і негативних петель зворотного зв'язку. Вплив зворотних зв'язків на стратегії атак і захисту. | 2 |
| **Тема 6. Стабільність кіберсистем та її порушення.** Моделювання стабільності та вразливості кіберсистем. Методи прогнозування розвитку кіберконфліктів. | 2 |
| **Тема 7. Інструменти моделювання системної динаміки.** Вивчення спеціалізованих програм для моделювання: Vensim, AnyLogic, Stella. | 2 |
| **Тема 8. Управління кіберконфліктами.** Розробка стратегій управління кіберконфліктами на основі моделювання. | 2 |
| **Загальна кількість годин** | **16** |

## Лабораторні заняття

| Теми лабораторних занять | Кількість годин | Вагові коефіцієнти $a$ |
|---|---|---|
| **Тема 1. Побудова базової моделі кіберконфлікту.** Введення в моделювання з використанням системної динаміки. | 7 | 0,2 |
| **Тема 2. Моделювання кіберзагроз.** Створення моделей типових кіберзагроз та їх наслідків. | 7 | 0,2 |
| **Тема 3. Симуляція кіберконфліктів за сценаріями.** Реалізація різних сценаріїв кіберконфліктів з використанням симуляції. | 6 | 0,2 |
| **Тема 4. Моделювання та аналіз петель зворотного зв'язку.** Вплив позитивних і негативних зворотних зв'язків на результат кіберконфлікту. | 6 | 0,1 |
| **Тема 5. Розробка стратегії управління кіберконфліктом.** Симуляція різних стратегій кіберзахисту та оцінка їхньої ефективності. | 6 | 0,1 |
| **Загальна кількість годин** | **32** | $\sum_{i=1}^{n} a_i = 0{,}8$ |

## Контрольні роботи

| Теми контрольних робіт | Вагові коефіцієнти $b$ |
|---|---|
| **Тема 1. Моделювання динаміки кіберзагроз та ефективності захисних механізмів.** Дослідження розвитку кіберзагроз у часі та оцінка ефективності заходів захисту за допомогою системної динаміки. Побудова моделей із петлями зворотного | 0,1 |

| | |
|---|---|
| зв'язку, симуляція впливу стратегій захисту на рівень інцидентів, пошук оптимальних рішень для зменшення ризику ескалації конфліктів. | |
| **Тема 2. Сценарії та стабільність кіберсистем у динамічних конфліктах.** Аналіз типових сценаріїв кіберконфліктів та дослідження стабільності кіберсистем за допомогою системної динаміки. Побудова системних діаграм ескалації, виявлення критичних вузлів і точок рівноваги, симуляція різних стратегій управління для підтримання стабільності та мінімізації наслідків атак. | 0,1 |
| **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 Основи системної динаміки в контексті кібербезпеки.** Петлі зворотного зв'язку, потоки та накопичувачі, моделювання поведінки складних систем. | 8 |
| **Тема 2. Моделювання поширення кібератак у складних мережах.** Динамічні моделі зараження, подібні до SIR-моделей, адаптовані для кіберзагроз. | 8 |
| **Тема 3. Моделі ескалації та деескалації кіберконфліктів між державами.** Фактори, що впливають на агресію, відповідь, порогові ефекти, перехід системи у хаотичний стан. | 7 |
| **Тема 4. Системно-динамічні моделі поведінки зловмисника.** Мотивація, ресурси, стратегія та адаптація хакера в часі. | 7 |
| **Тема 5. Моделювання ефективності кіберзахисту на рівні організації.** Взаємодія між інвестиціями в захист, людським фактором, технологіями та рівнем ризиків. | 7 |
| **Тема 6. Динаміка поширення фішингових кампаній та соціальної інженерії.** Поведінкові моделі користувачів, вплив інформаційної обізнаності, ефект масового впливу. | 7 |
| **Тема 7. Моделювання стійкості інформаційних інфраструктур.** Відновлення після атак, наявність резервів, затримки в реагуванні, ефект "порогу відмови". | 7 |
| **Тема 8. Кіберконфлікти в критичній інфраструктурі: сценарне моделювання.** Електромережі, транспорт, телеком. Взаємний вплив технічних та людських факторів. | 7 |
| **Тема 9. Моделювання інформаційних операцій та кіберпсихологічних впливів.** Динаміка чуток, інформаційних хвиль, маніпуляцій та їх вплив на поведінку груп. | 7 |
| **Тема 10. Використання програмних засобів системної динаміки (Vensim, Stella, AnyLogic) для моделювання кіберконфлікту.** Створення моделей, симуляції, аналіз чутливості, множинні сценарії. | 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. Sterman, John. Business Dynamics: Systems Thinking and Modeling for a Complex World. McGraw-Hill Education, 2000. [Електронний ресурс]. – Режим доступу : https://books.google.com.ua/books/about/Business_Dynamics.html?id=CCKCQgAACAAJ&redir_esc=y
2. Forrester, Jay W. Industrial Dynamics. MIT Press, 1961. [Електронний ресурс]. – Режим доступу : http://www.laprospective.fr/dyn/francais/memoire/autres_textes_de_la_prospective/autres_ouvrages_numerises/industrial-dynamics-forrester-1961.pdf
3. Ramin S. Esfandiari, Bei Lu Modeling and Analysis of Dynamic Systems, 2015. [Електронний ресурс]. – Режим доступу : https://ia903006.us.archive.org/34/items/CambridgeInternationalASAndALevelMathematicsPureMathematics1/Second_Edition_Modeling_and_Analysis_of.pdf

### Додаткова література

4. Richardson, George P. Feedback Thought in Social Science and Systems Theory. University of Pennsylvania Press, 1991. [Електронний ресурс]. – Режим доступу : https://books.google.com.ua/books/about/Feedback_Thought_in_Social_Science_and_S.html?id=Ey58AAAAIAAJ&redir_esc=y
5. Vensim Official Documentation. Vensim User's Guide. Ventana Systems, 2020. [Електронний ресурс]. – Режим доступу : https://vensim.com/
6. AnyLogic Documentation. AnyLogic in Practice: Model Development and Simulation. AnyLogic Software, 2018.

## 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:

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

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 |