**Силабус освітнього компонента**
Програма навчальної дисципліни

# Системно-динамічне моделювання кіберконфліктів

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Освітньо-професійна програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
2

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 "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 роботи, самостійна робота, консультації. Підсумковий контроль – 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 – 16 год., самостійна робота – 88 год.

### Передумови вивчення дисципліни (пререквізити)

Основи кібербезпеки, Технології програмування, 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 системної динаміки та моделювання кіберконфліктів.
Основи системної динаміки. Типові кіберконфлікти. Застосування системної динаміки у кібербезпеці.
Тема 2. Кіберзагрози та їх динаміка.
Види кіберзагроз. Моделювання кіберзагроз та їх впливу на системи.
Тема 3. Моделювання захисних механізмів у кіберпросторі.
Оцінка ефективності заходів кіберзахисту. Побудова моделей протидії кіберзагрозам.
Тема 4. Сценарії кіберконфліктів.
Аналіз типових сценаріїв кіберконфліктів. Моделювання динамічної ескалації кіберконфліктів.
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.
Тема 6. Стабільність кіберсистем та її порушення.
Моделювання стабільності та вразливості кіберсистем. Методи прогнозування розвитку кіберконфліктів.
Тема 7. Інструменти моделювання системної динаміки.
Вивчення спеціалізованих програм для моделювання: Vensim, AnyLogic, Stella.
Тема 8. Управління кіберконфліктами.
Розробка стратегій управління кіберконфліктами на основі моделювання..

### Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

### Теми лабораторних робіт

Тема 1. Побудова базової моделі кіберконфлікту.
Введення в моделювання з використанням системної динаміки.
Тема 2. Моделювання кіберзагроз.
Створення моделей типових кіберзагроз та їх наслідків.
Тема 3. Симуляція кіберконфліктів за сценаріями.
Реалізація різних сценаріїв кіберконфліктів з використанням симуляції.
Тема 4. Моделювання та аналіз петель зворотного зв'язку.
Вплив позитивних і негативних зворотних зв'язків на результат кіберконфлікту.
Тема 5. Розробка стратегії управління кіберконфліктом.
Симуляція різних стратегій кіберзахисту та оцінка їхньої ефективності.

### 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. 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

### 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;
•залік: 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 — Ольга КОРОЛЬ