СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Моделювання складних нелінійних процесів в кібербезпеці»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	магістр
	Освітня програма	Кібербезпека
	Тривалість викладання	3,4 чверті
	Заняття:	весняний семестр
	лекції:	2 години
	практичні заняття:	2 години
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=5376

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладачів:

Корнієнко Валерій Іванович	професор, д.т.н.
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/head.php
E-mail:	**korniienko.v.i@nmu.one**

1. Анотація до курсу

Наразі характерним є широке застосування методів нелінійної динаміки (теорії хаосу та фрактального аналізу) та методів систем штучного інтелекту (нейронних мереж, систем нечіткого висновку, еволюційного моделювання тощо) для моделювання складних процесів в кібербезпеці. Їх актуальність обумовлена, по-перше, спроможністю методів нелінійної динаміки більш узагальнено з єдиних позицій описувати складні процеси в системах різної природи, а, по-друге, здатністю інтелектуальних методів розв'язувати оптимізаційні задачі, що погано формалізуються.

Моделювання – найефективніший спосіб дослідження складних систем різного призначення, як на етапі їх проектування, так і в процесі експлуатації. Можливості розробки та вдосконалення IT-систем та проектів для кібербезпеки далеко не вичерпані, тому постійно з'являються найновіші методи та технології моделювання.

Послідовність вивчення матеріалу курсу «Моделювання складних нелінійних процесів в кібербезпеці» підпорядкована етапам процесу моделювання, основні з яких указуються усіма науковцями, що займаються проблемами моделювання. По-перше, це системний аналіз об'єкта дослідження та формулювання цілі та задачі дослідження, визначення змінних та параметрів моделі. По-друге – формалізація

моделі відомими засобами формального представлення. Реалізація моделі – найбільш відповідальний етап моделювання системи. Дослідження моделі – найбільш цікавий і творчий етап моделювання. Побудувати модель – тільки частина справи, уміти отримати результати моделювання – найважливіше. Отже, мистецтво дослідника полягає саме у тому, щоб здобути в процесі моделювання корисні, з огляду цілі моделювання, результати.

2. Мета та завдання курсу

Мета дисципліни – формування у студентів компетентностей щодо принципів побудови та оцінки моделей складних нелінійних процесів різного походження, що використовуються на різних етапах аналізу, розробки та застосування систем технічного захисту інформації, захисту в інформаційно-комунікаційних мережах та кібербезпеці.

.

Завдання курсу:

– ознайомити здобувачів вищої освіти із основами теорії систем;

– ознайомити здобувачів з застосуваннями теорії систем та особливостями складних систем;

– ознайомити здобувачів із математичними моделями систем та методами і моделями теорії оптимальних процесів;

– ознайомити здобувачів із особливостями моделювання нелінійних динамічних систем та систем із детермінованим хаосом;

– ознайомити здобувачів вищої освіти з фрактальним аналізом динамічних процесів;

– ознайомити здобувачів вищої освіти з основами частотно-часового аналізу сигналів, породжуваних нелінійними динамічними процесами;

– ознайомити здобувачів вищої освіти з практичними застосуваннями інтелектуальних методів при рішенні завдань в системах кібербезпеки;

– ознайомити здобувачів вищої освіти із програмним забезпеченням імітаційного моделювання процесів, що використовуються для технічного захисту інформації, захисту в інформаційно-комунікаційних мережах та кібербезпеці.

3. Результати навчання

Розробляти та удосконалювати сучасні інформаційні технології моделювання інформаційно-комунікаційних мереж та систем, математичні методи і моделі в сфері інформаційної та кібербезпеки.

Досліджувати, розробляти та використовувати методи та засоби криптографічного та технічного захисту інформації операційних процесів із використанням їх імітаційного моделювання для аналізу та оцінки ефективності їх використання в інформаційних системах.

Застосувувати інтелектуальні методи та засоби оптимізації, прогнозування та прийняття рішень з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах.

Розв’язувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням кращих практик моделювання нелінійних процесів в кібербезпеці.

Використовувати методи комп’ютерного моделювання для оцінювання, ідентифікації та прогнозування процесів, які стосуються інформаційної безпеки

та/або кібербезпеки.

Здійснювати моделювання процесів із використанням методів систем штучного інтелекту та нелінійної динаміки для дослідження та розробки методів та засобів інформаційної безпеки та/або кібербезпеки.

4. Структура курсу

ЛЕКЦІЇ **80**

І. Методи моделювання складних нелінійних процесів в кібербезпеці

1. Методи і моделі систем. Інформаційний підхід в теорії систем.
2. Застосування загальної теорії систем. Складні системи.
3. Математичні моделі систем керування.
4. Методи та моделі теорії оптимальних процесів.
5. Моделювання нелінійних процесів та детермінований хаос.
6. Фрактальні моделі нелінійних процесів.

ІІ. Оптимізація моделей складних нелінійних процесів та їх застосування в кібербезпеці

7. Реконструкція моделей нелінійних динамічних систем.
8. Фрактальний аналіз часових рядів.
9. Адаптивне прогнозування сигналів та стану об’єктів.
10. Структурно-параметрична ідентифікація та прогнозування нелінійних динамічних процесів.
11. Моделі моніторингу самоподібного трафіку в ІКМ для систем виявлення атак
12. Оцінювання, ідентифікація та прогнозування самоподібного трафіку в ІКМ для систем виявлення атак
13. Кіберфізична система моделювання захисту акустичної інформації від витоку
14. Інтелектуальне прогнозування мовного сигналу в системі конфіденційного зв’язку

ПРАКТИЧНІ ЗАНЯТТЯ **70**

І. Методи моделювання складних нелінійних процесів в кібербезпеці

1. Імітаційне моделювання супутникової системи зв’язку
2. Вейвлет перетворення векторних сигналів
3. Банки вейвлет фільтрів

ІІ. Оптимізація моделей складних нелінійних процесів та їх застосування в кібербезпеці

4. Оптимізація моделі адаптивною системою нечіткого висновку
5. Адаптивна нечітка оптимізація моделі динамічного нелінійного процесу
6. Нейромережева система оптимізації процеса з прогнозом

РАЗОМ **150**

5. Технічне обладнання та/або програмне забезпечення

Технічні засоби навчання: мультимедійні та комп’ютерні пристрої.

Програмні засоби дистанційної освіти: MS Office 365, MS Teams, дистанційна платформа Moodle.

Пакет прикладних програм Matlab&Simulink 2015 і вище (навчальна безкоштовна версія).

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 - 89	добре
60 - 73	задовільно
0 - 59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
53	42	30	5	**100**

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі іспиту. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

53 бали – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи.

7 балів – Достатня зрозумілість відповіді

5 бали – Добра зрозумілість відповіді

3 бали – Задовільна зрозумілість відповіді

0 балів – Незадовільна зрозумілість відповіді

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов’язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об’єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

7.6. Бонуси

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освіти буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на ваші університетські поштові скриньки. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни. За участь у анкетуванні здобувач вищої освіти отримує **5 балів**.

8 Рекомендовані джерела інформації

1. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в керуванні, кібербезпеці, телекомунікаціях: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна. – Міністерство освіти і науки України, Національний технічний університет «Дніпровська політехніка». – Дніпро, НТУ «ДП», 2020. – 531 с.

2. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. — К.: ІСЗЗІ КПІ ім. Ігоря Сікорського», 2018. — 297 с.

3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.

4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

5. Корнієнко В.І.. Теорія систем керування: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна, В.П. Щокін. – М-во освіти і науки України, Нац. гірн. ун-т. – Дніпро: НГУ, 2017. – 497 с. – ISBN 978-966-350-650-0. 2.

6. Gusev O.Yu. Theory of adaptive filtration: tutorial / O.Yu.Gusev, V.M.Gorev, V.I.Kornienko; Ministry of Education and Science of Ukrain, National Technical University “Dnipro polytechnic”.- Dnipro: NTU “DP”, 2019.- 156 p.