


## СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КІБЕРЗАХИСТУ»

|   |                              |                 |
|---|------------------------------|-----------------|
|  | <b>Ступінь освіти</b>        | магістр         |
|   | <b>Освітня програма</b>      | Кібербезпека    |
|   | <b>Тривалість викладання</b> | 1,2 чверті      |
|   | <b>Заняття:</b>              | осінній семестр |
|   | лекції:                      | 3 години        |
|   | практичні заняття:           | 2 години        |
| <b>Мова викладання</b>  | українська                   |                 |

Сторінка курсу в СДО НТУ «ДП»: <https://do.nmu.org.ua/course/view.php?id=2011>

Кафедра, що викладає

Безпеки інформації та телекомунікацій

**Інформація про викладачів:**



|                                      |   |
|--------------------------------------|---|
| <b>Котух Євген<br/>Володимирович</b> | професор, к.т.н.  |
| <b>Персональна сторінка</b>          | <a href="https://bit.nmu.org.ua/ua/pro_kaf/prepods/kotukh.php">https://bit.nmu.org.ua/ua/pro_kaf/prepods/kotukh.php</a> |
| <b>E-mail:</b>                       | <a href="mailto:kotukh.e.v@nmu.one">kotukh.e.v@nmu.one</a>  |



|  |   |
|--|---|
| <b>Герасіна<br/>Олександра<br/>Володимирівна</b> | доцент, к.т.н.  |
| <b>Персональна сторінка</b>                      | <a href="https://bit.nmu.org.ua/ua/pro_kaf/prepod/s/gerasina.php">https://bit.nmu.org.ua/ua/pro_kaf/prepod/s/gerasina.php</a> |
| <b>E-mail:</b>                                   | <a href="mailto:herasina.o.v@nmu.one">herasina.o.v@nmu.one</a>  |

### 1. Анотація до курсу

Наразі характерним є широке застосування методів систем штучного інтелекту (нейронних мереж, систем нечіткого висновку, еволюційного моделювання, агентських алгоритмів оптимізації) для здійснення наукових та/або прикладних досліджень у галузі інформаційної безпеки та/або кібербезпеки.

Їх актуальність обумовлена здатністю інтелектуальних методів розв'язувати оптимізаційні задачі, що погано формалізуються, а також використанням ефективних і універсальних апроксиматорів (нейронних мереж та систем нечіткого висновку).

## **2. Мета та завдання курсу**

**Мета дисципліни** – формування у студентів компетентностей щодо принципів використання інтелектуальних методів систем штучного інтелекту в системах кіберзахисту.

### **Завдання курсу:**

- ознайомити здобувачів вищої освіти із основами технології штучних нейронних мереж та їх ефективністю;
- ознайомити здобувачів вищої освіти з основами нечіткої логіки, алгоритмами побудови систем нечіткого висновку, алгоритмами нечіткої кластеризації; гібридними нейронечіткими мережами, а також із ефективністю усіх вищевказаних систем;
- ознайомити здобувачів вищої освіти із методами еволюційного моделювання (у тому числі із методами групового урахування аргументів);
- ознайомити здобувачів вищої освіти із агентськими алгоритмами оптимізації (мурашиними та бджолиними);
- ознайомити здобувачів вищої освіти з прикладами застосування інтелектуальних методів при рішенні завдань в кібербезпеці;
- ознайомити здобувачів вищої освіти із програмним забезпеченням імітаційного моделювання інтелектуальних методів систем штучного інтелекту, що використовуються у галузі кібербезпеки.

## **3. Результати навчання**

Застосовувати методи систем штучного інтелекту для розробки та удосконалення сучасні інформаційні технологій та математичних методів і моделей інтелектуальних систем в сфері інформаційної безпеки та/або кібербезпеки.

Обґрунтовувати, аналізувати і розробляти адекватні інтелектуальні методи для систем кіберзахисту.

Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних інтелектуальних методів систем штучного інтелекту.

Здійснювати дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних інтелектуальних методів моделювання складних процесів та систем штучного інтелекту.

## **4. Структура курсу**

### **ЛЕКЦІЇ**

#### **Інтелектуальні методи обробки інформації.**

1. Основи технології штучних нейронних мереж.
2. Навчання нейронних мереж.
3. Архітектури нейронних мереж. Ефективність нейронних мереж
4. Нечіткі множини.
5. Нечіткі змінні та відношення. Системи нечіткого висновку.
6. Нечітка кластеризація. Ефективність систем з нечіткою логікою. Нейронечіткі мережі.

7. Біологічні передумови й загальна схема еволюційних алгоритмів. Генетичні алгоритми.
8. Еволюційна стратегія. Еволюційне програмування. Диференціальна еволюція. Метод групового урахування аргументів.
9. Алгоритми оптимізації роєм часток.
10. Мурашина оптимізація.
11. Оптимізація бджолиним роєм.

#### **Застосування інтелектуальних методів в кібербезпеці.**

12. Оцінка систем захисту інформації від витоку.
13. Методика нечіткої оцінки технічного стану комп'ютерної системи в задачах інформаційної безпеки.
14. Методика виявлення DoS-атак в інформаційно-комунікаційних мережах з використанням штучних нейронних мереж.
15. Виявлення фішингових URL-адрес за допомогою алгоритмів нечіткої кластеризації із глобальною оптимізацією.

### **ПРАКТИЧНІ ЗАНЯТТЯ**

1. Нейромережева класифікація даних.
2. Навчання нейронних мереж за методом зворотного поширення похибки.
3. Нейромережевий амплітудний детектор.
4. Кластеризація даних методами нечіткої логіки.
5. Прогнозуючий нечіткий фільтр.
6. Адаптивне придушення завад методом нечіткої логіки.

#### **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     | <b>100</b> |

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами задачі 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 (вигадкування 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](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 відбутись 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. Глибовець М. М. Штучний інтелект : підручник для студ. вищих навч.закладів / М. М. Глибовець, О.В. Олецкий. – К. : КМ Академія, 2002. – 369 с.

3. 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.
4. Зайченко, Ю.П. Нечіткі моделі і методи в інтелектуальних системах. - К: Слово, 2008. - 344 с.
5. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.
6. 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.
7. Nelles O. Nonlinear System Identification: From Classical Approaches to Neural and Fuzzy Models / O. Nelles. – Berlin: Springer, 2001. – 785 pp.