Харківський національний університет радіоелектроніки

Центр післядипломної освіти

ЗАТВЕРДЖУЮ

Заступник директор ЦПО

_____Марія ШИРОКОПЕТЛЄВА

“_____”_____ 2024 р.

НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН

Підвищення кваліфікації за курсом

Гібридні загрози та штучний інтелект

Форма навчання – денна з використанням
дистанційних технологій

Термін навчання - 2 місяця

Загальний обсяг – 90 годин (3 ЄКТС)

Харків 2024

Структура курсу

Гібридні загрози та штучний інтелект

№	Найменування тем	Всього, годин	Аудиторні, годин	Консультації, годин	Самостійна робота, годин
1	Нова картина глобальної безпеки: гібридні війни, гібридні загрози.	7	1	2	4
2	Вплив ШІ на безпековий ландшафт: використання ШІ для створення загроз, посилення ролі цифрового простору у гібридних конфліктах.	7	1	2	4
3	Сучасні інтелектуальні моделі та їхні вразливості	10	1	4	5
4	ШІ-інструменти в кібербезпеці: атрибутування атак, автоматизоване виявлення ворожої діяльності.	10	1	4	5
5	Елементи теорії ігор в кібербезпеці	7	1	2	4
6	Змагальне машинне навчання (Adversarial ML): змагальні (adversarial) атаки (типи, визначення, наслідки, контрзаходи).	10	1	4	5
7	Безпека інтелектуальних систем	9	1	4	4
8	Стійкість машинного навчання (deep learning) до атак.	10	1	4	5
9	Інформаційний менеджмент у гібридній війні: автоматичне виявлення дезінформації, автоматизована верифікація інформації.	10	1	4	5
10	Підсумковий контроль, залік (презентація виконаних завдань)	10	1	4	5
	Всього	**90**	**10**	**34**	**46**

Доцентка кафедри штучного інтелекту Марія ГОЛОВЯНКО

Заступник директора ЦПО Марія ШИРОКОПЕТЛЄВА

ПОЯСНЮВАЛЬНА ЗАПИСКА

до навчально-тематичного плану підвищення кваліфікації з курсу

«Гібридні загрози та штучний інтелект»

Призначення курсу «Гібридні загрози та штучний інтелект» – надати теоретичні знання і практичні навички, необхідні для попередження гібридних впливів, виявлення гібридних кампаній, планування і реалізацію ефективних відповідей на них в сфері штучного інтелекту.

«Гібридні загрози та штучний інтелект» – це новаторський курс, розроблений в рамках проєкту Еразмус+ WARN «Академічна протидія гібридним загрозам» 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP (https://warn-erasmus.eu).

Дисклаймер: цей проєкт фінансується за підтримки Європейської Комісії. Дана публікація відображає лише погляди автора, і Комісія не несе відповідальності за будь-яке використання інформації, що міститься в ній.

Disclaimer: this project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Після закінчення курсу слухач **ПОВИНЕН ЗНАТИ**:

- ключові поняття галузі штучного інтелекту, пов'язані з гібридними загрозами;
- місце кібер-домену в концептуальній моделі гібридних загроз та взаємозв'язок інструментів штучного інтелекту з іншими елементами моделі;
- основні інструменти штучного інтелекту для протидії гібридним загрозам;
- особливості роботи інтелектуальних систем в умовах гібридних загроз;
- основні підходи, теорії, моделі та методи для захисту та протидії гібридним загрозам в штучному інтелекті.
- основні підходи до створення стійкої інформаційної інфраструктури та інформаційного менеджменту

Після закінчення курсу слухач **ПОВИНЕН ВМІТИ:**

- виявляти вразливості систем штучного інтелекту;
- виявляти, ідентифікувати та візуалізувати гібридні загрози у цифровому просторі за допомогою інструментів штучного інтелекту;
- розробляти інструменти штучного інтелекту для виявлення, ідентифікації та візуалізації гібридних загроз;
- створювати механізми захисту та протидії гібридним загрозам в штучному інтелекті;

- адаптувати інформаційну екосистему до складних і непередбачуваних ситуацій, спричинених гібридними загрозами.

Курс передбачає проведення аудиторних занять, консультацій та самостіної роботи з використанням комп'ютерної техніки та доступом до Інтернет.

На реалізацію програми відводиться 90 годин, з них 10 годин аудиторних занять, 34 години – консультацій (зокрема – для індивідуального засвоєння теоретичного матеріалу, для допомоги у виконання практичних завдань та для допомоги у підготовці підсумкової презентації результатів) та 46 годин самостійної роботи.

В освітньому процесі використовується спеціалізована навчальна лабораторія з протидії гібридним загрозам, що була створена та обладнана в межах реалізації проєкту Еразмус+ КА2 «WARN: Academic Response to Hybrid Threats» (610133-EPP-1-2019-1-FI–EPPKA2–CBHE– JP), який фінансується програмою Erasmus+ Європейського Союзу. Лабораторія є складовою міжфакультетського хабу ХНУРЕ з протидії гібридним загрозам, а також учасником міжгалузевого середовища з протидії гібридним загрозам WARN.

Після успішного освоєння курсу та захисту випускної роботи слухачі отримують свідоцтво про підвищення кваліфікації державного зразку.

НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ

Основна література

1. Гришко С., Головянко М., Титаренко М., Чех М., Василиця О., Ланюк Є., Засадко В., Карпенко О., Завгородній В., Балашов Е., Рева Т., Копієвська О., Білоконь М., Величко Л., Докашенко Г., Концур В., Наумов І. (2021). Глосарій з гібридних загроз. URL: https://warn-erasmus.eu/ua/glossary/

Додаткова література

1. Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305
2. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023. 124 p. doi:10.2760/37899, JRC129019.

3. Comiter, M. (2019). Attacking artificial intelligence. *Belfer Center Paper*, *8*, 2019-08.
4. Mazzucchi, N. (2022). Hybrid CoE Paper 14. AI-based technologies in hybrid conflict: The future of influence operations. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf
5. Golovianko, M., Terziyan, V., Branytskyi, V., & Malyk, D. (2023). Industry 4.0 vs. Industry 5.0: Co-existence, transition, or a hybrid. *Procedia Computer Science*, *217*, 102-113.
6. Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., & Titova, L. (2022). Hybrid threats against Industry 4.0: adversarial training of resilience. In *E3S Web of Conferences*. EDP Sciences.

Доцентка кафедри штучного інтелекту Марія ГОЛОВЯНКО