Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут *електронних та інформаційних технологій*
Кафедра *кібербезпеки та математичного моделювання*

СИЛАБУС
Інформаційно-психологічне протиборство

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____Ткач Ю.М._____
(підпис) (прізвище та ініціали)

«__26___» ____08___ 2024 р.

Розробник (-и): Ткач Юлія Миколаївна, завкафедри КБММ, д.пед.н., к.т.н., проф. _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри _____
(назва кафедри)

Протокол від «__26___»__08_____2024р. №__7__

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*вибіркова*
Мова викладання	українська
Рік навчання та семестр	1 рік, 2 семестр 125 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Ткач Юлія Миколаївна, завкафедри КБММ, д.пед.н., к.т.н., проф.
Профайл викладача (-ів)	Web: https://mmi.stu.cn.ua/personal-kafedry/ ORCID: 0000-0002-8565-0525
Контакти викладача	Чернігів, вул. Шевченка, 95, корп.1, каб. 108; E-mail: tkachym@stu.cn.ua

2. Анотація курсу. Курс "Інформаційно-психологічна протидія в кіберпросторі" спрямований на формування у студентів знань та навичок, необхідних для аналізу та оцінки інформаційно-психологічних загроз у кіберпросторі, розробки стратегій протидії, а також застосування сучасних методів інформаційної безпеки. Дисципліна охоплює теоретичні засади інформаційної боротьби, кіберпсихологію, методи інформаційного впливу та захисту інформації.

Посилання на курс в MOODLE: https://eln.stu.cn.ua/course/view.php?id=4448

3. Мета та цілі курсу.

Формування у студентів професійної компетентності щодо інформаційно-психологічного впливу в кіберпросторі, методів протидії інформаційним загрозам та забезпечення інформаційної безпеки на рівні особистості, суспільства та держави.

Завдання курсу

- Ознайомлення з основними поняттями та концепціями інформаційно-психологічної війни та кіберпсихології.
- Аналіз методів інформаційного впливу та інформаційних атак у кіберпросторі.
- Вивчення механізмів психологічного впливу та маніпулятивних технологій у цифровому середовищі.
- Опанування методів захисту від інформаційно-психологічних загроз.
- Розвиток навичок аналізу, прогнозування та протидії інформаційним атакам.
- Ознайомлення з правовими аспектами інформаційної безпеки.
- Використання інструментів та технологій для моніторингу та виявлення інформаційних загроз.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Здатність проводити дослідження на відповідному рівні.

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу

КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки

4. Результати навчання.

За результатами вивчення курсу студенти повинні:

Знати:

- Основи інформаційно-психологічної безпеки.
- Класифікацію загроз інформаційно-психологічної війни.
- Методи аналізу та оцінки інформаційних атак.
- Механізми інформаційного впливу та дезінформації.
- Стратегії протидії інформаційним загрозам у кіберпросторі.
- Законодавчу базу щодо інформаційної безпеки та протидії кібератакам.

Вміти:

- Ідентифікувати інформаційні загрози та оцінювати їхній вплив.
- Використовувати методи аналізу інформаційних атак та їх наслідків.
- Розробляти стратегії захисту від інформаційно-психологічних атак.
- Застосовувати сучасні технології моніторингу та аналізу інформаційних потоків.
- Виявляти маніпулятивний контент та інформаційні операції у медіа та соціальних мережах.
- Використовувати правові механізми захисту інформаційної безпеки.

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 2- Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах;

5. Пререквізити. Дисципліна є складовою частиною вибіркових дисциплін циклу професійної підготовки. Вивчення курсу передбачає наявність систематичних та ґрунтовних знань із курсу – ОК 4. Методологія та організація наукових досліджень.

6. Обсяг курсу. Зазначте загальну кількість кредитів, кількість занять та годин самостійної роботи.

Вид заняття	Загальна кількість годин
Лекції	16/6
Практичні заняття	14/6
Самостійна робота	90/108
Індивідуальне завдання –	
Всього кредитів – *вказати кількість кредитів*	4

7. Тематика курсу.

Змістовий модуль 1. Основи інформаційно-психологічної безпеки

Тема 1. Вступ до інформаційно-психологічної безпеки
Основні поняття та визначення. Інформаційна війна як глобальне явище. Види інформаційно-психологічного впливу.

Тема 2. Теоретичні засади інформаційних воєн
Історичний розвиток інформаційних війн. Стратегії інформаційного протиборства. Роль медіа у веденні інформаційної війни.

Тема 3. Методи та засоби ведення інформаційно-психологічних операцій
Основні методи психологічного впливу. Тактики інформаційно-психологічного протиборства. Роль соціальних мереж у інформаційній війні.

Тема 4. Інформаційно-психологічні загрози та їхній вплив на суспільство
Типи інформаційних загроз. Вплив дезінформації на громадську думку. Маніпулятивні технології у цифровому середовищі.

Змістовий модуль 2. Інформаційна безпека та протидія інформаційним загрозам

Тема 5. Маніпулятивні технології та інформаційні атаки
Інформаційні маніпуляції у соціальних мережах. Дезінформація та пропаганда. Фейкові новини та методи їх розпізнавання.

Тема 6. Захист від інформаційно-психологічних впливів
Методи виявлення та блокування шкідливого контенту. Інструменти протидії інформаційним атакам. Психологічні аспекти інформаційного впливу.

Тема 7. Методи кіберпсихологічного аналізу
Методи моніторингу та аналізу інформаційного простору. Соціально-психологічні аспекти інформаційної війни. Використання штучного інтелекту для аналізу інформаційних загроз.

Тема 8. Правові аспекти інформаційної безпеки
Законодавче регулювання кібербезпеки. Етичні питання інформаційної війни. Міжнародне право у сфері інформаційної безпеки.

8. Система оцінювання та вимоги .

Загальна система оцінювання курсу	● Оцінювання курсу відбувається за 100 бальною шкалою. Протягом семестру здобувач вищої освіти може набрати 60 балів: практичні/лабораторні оцінюється в 20/10 балів, відповіді – 8/18 балів, іспит – 40 балів. Допоміжні бали виставляються за виконання макетів, виступи на конференціях, написання тез та статей.
Вимоги до РГР, КР, КП тощо	● Виконання модульних контрольних робіт ● Щонайменше за результатами контролю протягом семестру ЗВО повинен отримати 40 балів
Практичні (лабораторні) заняття	Модуль за тематичним планом дисципліни та форма контролю: ● Кількість балів - 0…60: ● 1. Виконання практичних/лабораторних робіт 0…20/10 ● 2. Самостійна робота 0…8/18

	• 3. Повнота відповідей на запитання на лекціях 0…2
Умови допуску до підсумкового контролю	• Оцінювання курсу відбувається за 100 бальною шкалою. Протягом семестру здобувач вищої освіти може набрати 60 балів: практичні/лабораторні оцінюється в 20/10 балів, відповіді – 8/18 балів, іспит – 40 балів. Допоміжні бали виставляються за виконання макетів, виступи на конференціях, написання тез та статей.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1.		
1	Повнота відповідей на запитання на лекціях	0…2
2	Результати захисту практичних робіт	0…20/10
3	Самостійна робота	0…8/18
Змістовий модуль 2.		
1	Повнота відповідей на запитання на лекціях	0…2
2	Результати захисту практичних робіт	0…20/10
3	Самостійна робота	0…8/18
Усього поточний і проміжний модульний контроль		**0…60**
Семестровий контроль (Екзамен/диференційований залік/залік)		**0…40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		

66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення (за необхідності**).**

10. Політики курсу. У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ “Чернігівська політехніка”». Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний диференційований залік складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на

замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Базова література

1. **Корченко А. Г., Дубов Д. В., Потій О. В.** (2021). *Кібербезпека та інформаційна війна: сучасні виклики та стратегії протидії*. Київ: Національний інститут стратегічних досліджень.

2. **Snegovaya, M.** (2020). *Weaponizing information: The Russian way of information warfare*. Center for European Policy Analysis.

3. **Бакалінський О. В., Мялковський Д. В.** (2022). *Інформаційно-психологічні операції у сучасних конфліктах*. Київ: Інститут проблем національної безпеки.

4. **Prier, J.** (2019). *Commanding the trend: Social media as information warfare*. Strategic Studies Quarterly, 13(4).

5. **Shcyhol, Y., Korchenko, O.** (2023). *Cyber and Information Security: Psychological Aspects of Hybrid Warfare*. Kyiv: ДУТ.

6. **Nissen, T. E.** (2020). *The Weaponization of Social Media*. Royal Danish Defence College.

7. **Дубов Д. В.** (2021). *Інформаційна безпека України: виклики гібридної війни*. Київ: НІСД.

8. **Golovchenko, Y., Hartmann, M., Adler-Nissen, R.** (2020). *State, media and civil society in the information warfare*. International Affairs, 96(5).

9. **Benkler, Y., Faris, R., Roberts, H.** (2020). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.

10. **Семенченко А. І.** (2023). *Методи кіберпсихологічного аналізу інформаційних загроз*. Київ: КНУ ім. Шевченка.

Допоміжна література

1. **Rid, T.** (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.

2. **McKay, S., Tenove, C.** (2021). *Disinformation as a Threat to Deliberative Democracy*. Political Communication, 38(3).

3. **Бондаренко О. В.** (2022). *Маніпулятивні технології у цифровому середовищі*. Харків: ХНУ ім. В. Н. Каразіна.

4. **Helmus, T. C., Bodine-Baron, E.** (2020). *Russian Social Media Influence: Understanding Disinformation Tactics*. RAND Corporation.

5. **Яремчук С. В.** (2019). *Психологічні аспекти інформаційно-психологічної безпеки*. Львів: ЛНУ ім. Франка.

6. **Woolley, S. C., Howard, P. N.** (2019). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford University Press.

7. **Мялковський Д. В.** (2023). *Правові засади протидії інформаційним загрозам*. Київ: Юрінком Інтер.

8. **Wardle, C., Derakhshan, H.** (2021). *Information Disorder: Disinformation, Misinformation and Malinformation*. Council of Europe Report.

9. **Ліпкан В. А.** (2020). *Теорія національної безпеки України: інформаційний вимір*. Київ: КНТ.

10. **Hutchings, S., Szostek, J.** (2022). *Dominant Narratives in Russian Media: Information Warfare in Practice*. Journal of Communication, 72(1).

17 Інформаційні ресурси

1. http://www.library.snu.edu.ua/ – Наукова бібліотека.
2. https://nlu.org.ua/– Національна бібліотека України імені Ярослава Мудрого.
3. https://www.researchgate.net/– науковий портал.
4. http://www.nbuv.gov.ua/ – Національна бібліотека ім. В.І. Вернадського
5. Система дистанційного навчання НУ «Чернігівська політехніка». Курс: **Інформаційно-психологічне протиборство**. – [Електронний ресурс]. – Режим доступу: https://eln.stu.cn.ua/course/view.php?id=4448