

**НАЦІОНАЛЬНА АКАДЕМІЯ КЕРІВНИХ КАДРІВ КУЛЬТУРИ І МИСТЕЦТВ
ЦЕНТР НЕПЕРЕРВНОЇ КУЛЬТУРНО-МИСТЕЦЬКОЇ ОСВІТИ**

«ЗАТВЕРДЖУЮ»

Перший проректор
з науково-педагогічної роботи
Людмила СТЕПАНЕНКО
«28» серпня 2024 року

ГІБРИДНІ ЗАГРОЗИ ТА КОМПЛЕКСНА БЕЗПЕКА

**Програма підвищення кваліфікації керівників та спеціалістів
закладів культури**

Форма навчання	очно/заочна
Навчальний рік	2024/2025
Кількість кредитів ECTS	2,5
Мова викладання, навчання та оцінювання	українська
Форма підсумкового контролю	залік

Розробник: Рева Тетяна Сергіївна

Київ – 2024

Розробник: РЕВА Тетяна Сергіївна, кандидат політичних наук, доцент.

ПОГОДЖЕНО:

Директорка Центру неперервної
культурно-мистецької освіти
кандидат педагогічних наук, доцент

Ірина ШЕВЧЕНКО

СХВАЛЕНО:

В.о. зав. кафедри арт-менеджменту та
івент технологій, доктор наук з
соціальних комунікацій, професор,
академік ГО "Національна академія
наук вищої освіти України", член
спілки документознавців України

Вікторія ДОБРОВОЛЬСЬКА

Протокол № 1 від «26» серпня 2024 р.

Схвалено Радою якості освіти Академії

Протокол від «28» серпня 2024 р. № 1

Затверджено Вченою радою Академії протокол від «29» серпня 2024 р. № 1

© Рева Т.С., 2024

© НАКККіМ, 2024

1. Анотація (опис) навчальної програми (у т.ч. міждисциплінарні зв'язки):

«Гібридні загрози та комплексна безпека» є програмою для підвищення кваліфікації працівників культури, керівників структурних підрозділів, директорів та заступників директорів базової мережі закладів культури та спрямована на підвищення рівня їхніх інтегральної, загальних та професійних компетентностей.

Програму підвищення кваліфікації «Гібридні загрози та комплексна безпека» розроблено з метою формування у працівників культури компетентностей, що пов'язані з процесами прогнозування, виявлення та аналізу гібридних загроз (далі – HTs) та їх впливу на соціокультурну діяльність. На теоретико-практичних матеріалах ознайомити слухачів із теоріями гібридних загроз, а також проектування аналізу та виявлення гібридних загроз на соціокультурне середовище.

Програму підвищення кваліфікації «Гібридні загрози та комплексна безпека» передбачає набуття професійних знань з теорії гібридних загроз, а також застосування методик їх аналізу, а саме – PMESII-матриця та Dilemma-game. Застосовувати виявлені та самостійно осмислені теорії в їх практичному професійному використанні.

Програма підвищення кваліфікації «Гібридні загрози та комплексна безпека» розроблена в рамках реалізації міжнародного проекту Erasmus+ WARN «Academic Response to Hybrid Threats» (610133-EPP-1-2019-1-FI-EPPKA2-SBHE-JP), що фінансується за підтримки Європейської Комісії.

Мета програми – ознайомлення здобувачів з концепціями гібридних загроз, їх проявах у основних доменах функціонування суспільства, культурі зокрема, інструментарієм HTs, системою безпекового ландшафту та протидії гібридним загрозам.

2. Завдання програми:

- опанувати теоретичні засади з теорії гібридних загроз та гібридних війн;
- набути знання та навички, необхідні для розуміння, аналізу та реагування на HTs в професійній діяльності та громадському житті;
- оволодіння вміннями та методикою, необхідних для виконання організаційних, аналітичних та консультативних функцій щодо ідентифікації та протидії HTs і забезпечення комплексної безпеки на національному й міжнародному рівні;
- набути знання щодо аналізу та виявлення гібридних загроз у соціокультурному просторі на локальному, глокальному та глобальному рівнях.

3. Програма забезпечує набуття таких компетентностей:

інтегральна компетентність: здатність розв'язувати складні задачі і проблеми в професійній діяльності.

загальні: здатність генерувати нові ідеї (креативність); здатність працювати в міжнародному контексті.

фахові: Здатність до практичної адаптації науковообґрунтованих соціокультурних практик в їх глобальному, глокальному і локальному вимірах; здатність швидко адаптуватися до викликів часу до специфічних умов і напрямів професійної діяльності; здатність застосовувати креативні технології на практиці.

3. Результати навчання за програмою:

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання (за необхідності)	Відсоток у підсумковій оцінці
Код	Результат навчання			
РН1.	Відшукувати, аналізувати та оцінювати інформацію, необхідну для постановки і вирішення як професійних завдань так і особистісного розвитку, використовувати на практиці фаховий науково-термінологічний апарат, вміти представляти підсумки виконаної роботи.	Лекційне заняття Практичне заняття	Перевірка виконання завдань	25
РН2.	Здійснювати професійну діяльність з дотриманням вимог чинного законодавства.	Лекційне заняття Практичне заняття	Перевірка виконання завдань	25
РН3.	Розуміти комплексну природу, складність, логіку і закономірності гібридних загроз, виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії.	Лекційне заняття Практичне заняття	Перевірка виконання завдань	25
РН4.	Створювати сприятливе культурно-мистецьке середовище з адаптивними крос-культурними, соціокультурними практиками та дієвою системою реагування на гібридні виклики.	Лекційне заняття Практичне заняття	Перевірка виконання завдань	25

4. Співвідношення результатів навчання із програмними результатами навчання (необов'язково для вибіркових дисциплін, які не входять до блоків спеціалізації)

5. Схема формування оцінки (згідно з п.7 «Положення про організацію освітнього процесу в НАКККіМ» від 16 грудня 2015 р.):

7.1. Форми оцінювання слухачів:

- поточне оцінювання:

1. Оцінювання роботи під час практичного заняття з теми 2: 10 балів*/ 5 балів.
2. Оцінювання роботи під час семінарського заняття з теми 3: 10 балів/ 10 балів
3. Оцінювання роботи під час практичного заняття з теми 4: 15 балів/ 10 балів.
4. Оцінювання роботи під час практичного заняття з теми 5: 15 балів/ 10 балів.
5. Оцінювання роботи під час практичного заняття з теми 6: 10 балів/ 5 балів.
6. Оцінювання роботи під час практичного заняття з теми 7: 10 балів/ 5 балів.
7. Оцінювання роботи під час практичного заняття з теми 8: 10 балів/ 5 балів.

8. Оцінювання роботи під час практичного заняття з теми 9: 10 балів/ 5 балів.

9. Оцінювання роботи під час практичного заняття з теми 10: 10 балів/ 5 балів.

* максимальний бал/ пороговий бал для отримання позитивної оцінки з відповідної форми контролю.

- **підсумкове оцінювання:** залік.

7.2. Організація оцінювання:

Контроль за якістю навчання слухача здійснюється за 100-бальною системою. Загальну кількість балів формують бали, отримані з усіх тем, змістових розділів: бали, отримані за практичні роботи, презентації тощо; бали, отримані за роботу на семінарських заняттях, а також бали, що отримані за підсумкову роботу (залік).

У випадку відсутності слухача з поважних причин, відпрацювання та передачі контрольних робіт здійснюються у відповідності до «Положення про організацію освітнього процесу у НАКККіМ» від 16 грудня 2015 р.

Залік виставляється за результатами роботи впродовж навчання за програмою. Слухач, який набрав суму залікових балів (60) має право отримати підсумкову оцінку за результатами контролю. Слухачі, які набрали протягом всієї програми менше 60 балів, обов'язково складають залік.

7.3. Шкала відповідності оцінок

Оцінка за шкалою НАКККіМ (бали)	Оцінка за чотирибальною шкалою	Оцінка за шкалою ЄКТС
90-100	Відмінно	A
82-89	Добре	B
74-81		C
64-73	Задовільно	D
60-63		E
35-59	Незадовільно	FX
1-34		F

ТЕМАТИЧНИЙ ПЛАН ЗАНЯТЬ
для підвищення кваліфікації керівників та спеціалістів
закладів культури за програмою «Гібридні загрози та комплексна безпека»

№ п/п	Назва розділів, тем	Всього Годин	Види занять та кількість годин			
			Лекції	Практичні	Самостійна робота	Контроль знань
1	Розвиток концепту гібридних загроз у ландшафті прийняття рішень	10	2	4	4	
2	Гібридні загрози: сутність та головні риси	6	2	2	2	Контрольна робота
3	Державні та недержавні актори гібридних загроз	6	2	4		Контрольна робота
4	Комплексна модель гібридних загроз та її інструменти	8	2	2	4	Контрольна робота
5	Інструменти гібридних загроз у інформаційному домені. Міфодизайн.	10	4	4	2	Контрольна робота
6	Культурний домен та його вразливості	12	4	4	4	Контрольна робота
7	ПВЕСІІ спектр / PMESII spectrum	8	2	4	2	Контрольна робота
8	Головні фази розвитку та функціонування гібридних загроз	4	2	2		Контрольна робота
9	Формуванням громадської стійкості як основний інструмент протидії гібридним загрозам	4	2	2		Контрольна робота

10	Культурно-мистецькі проєкти як інструмент протидії гібридним загрозам	4	-	4		Контрольна робота
	Залік, консультація	3				
	Разом	75	22	32	18	

Загальний обсяг 75 год., в тому числі:

Лекцій – 22 год.

Практичних (ввз) – 32 год.

Самостійна робота – 18 год.

Консультація, залік – 3 год.

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО САМОСТІЙНОЇ РОБОТИ СЛУХАЧІВ

Самостійна робота слухачів є одним з основних засобів оволодіння навчальним матеріалом у час, вільний від занять. Упровадження в практику навчальної програми різноманітних форм самостійної роботи активно сприяє модернізації навчального процесу шляхом подолання протиріч між трансляцією знань та їхнім засвоєнням у взаємозв'язку теорії та практики.

Головною метою самостійної роботи є закріплення, розширення та поглиблення набутих у процесі роботи знань, умінь і навичок, а також самостійне вивчення та засвоєння нового матеріалу.

Самостійна робота слухачів за програмою «Гібридні загрози та комплексна безпека» передбачена до кожної теми курсу, зміст якої полягає в таких положеннях:

- самостійне вивчення теоретичних тем;
- самостійна робота із джерелами з метою кращого засвоєння програмного матеріалу;
- підготовка теоретичних повідомлень, інформаційних довідок;
- підготовка вибіркового дослідного завдання на базі критичного огляду наукових публікацій, розроблення пропозицій щодо вирішення актуальних проблем або прогнозів за обраною тематикою.

Одним із видів самостійної роботи є опрацювання матеріалу, визначення головного в змісті лекції, засвоєння її основних моментів. Для систематизації отриманих знань за програмою до кожної наступної теми слід ретельно готуватись: систематично опрацювати матеріал попередньої лекції та рекомендовану літературу, повторювати пройдений матеріал. Основні види самостійної роботи слухачів з дисципліни: опрацювання лекційного матеріалу і рекомендованої літератури; самоконтроль рівня засвоєння програмного матеріалу; підготовка відповідей.

МЕТОДИ НАВЧАННЯ

Використання відповідних методів навчання у процесі викладання навчальної дисципліни «Гібридні загрози та комплексна безпека» зумовлено пізнавальним і формуючим значенням цієї дисципліни та її місцем у системі підвищення кваліфікації фахівців, а також метою і завданнями її вивчення. У процесі засвоєння матеріалів програми доцільно використовувати рекомендації зазначені у посібнику *«Методика навчання в умовах гібридних загроз: посібник / Е. Балашов, М. Білоконь, Т. Борозенцева, М. Головянко, С. Гришко, Т. Жовтенко та ін. – Харків: ТОВ "ТЕХНО-ЛОГІЧНИЙ ЦЕНТР ГРУП", 2023. – 84 с.»* <https://sciencebookgroup.org/catalog/view/338/533/2228>

Рекомендовані джерела:

Публікації науково-педагогічного працівника за програмою:

1. Рева Т. С. Глосарій з гібридних загроз / упоряд. С. В. Гришко та ін. ; за заг. ред. С. В. Гришко. 2021. 113 с.
2. Рева Т. С. Гібридні загрози та гібридні війни: сутність та аспекти взаємодії // Вісник Львівського університету. Філософсько-політологічні студії: зб. наук. праць. Львів, 2022. № 40. С. 186-191. URL: http://fps-visnyk.lnu.lviv.ua/archive/40_2022/24.pdf
3. Рева Т. С. Культурна травма у концепції соціальних змін Пйотра Штомпки // Вісник Національної академії керівних кадрів культури і мистецтв, 2022. № 2. С. 59-63 URL: <http://journals.uran.ua/visnyknakkkim/article/view/262207>
4. Рева Т. С. Культурні цінності як інструмент гібридних загроз. Новітні дослідження культури і мистецтва: пошуки, проблеми, перспективи : матеріали Всеукр. наук.-практ. конф. / М-во культ. України та інформ. політики ; Нац. акад. кер. кадрів культ. і мистец. ; Наук. тов. студ., асп., доктор. і молод. вч. (Київ, травень). Київ: НАКККіМ, 2023. 138-140 https://nakkkim.edu.ua/images/vidannya/Konferencii/Tezy_18_05_2023_1.pdf#page=138
5. Рева Т. С. Сміхтивізм: темний і світлий бік в інформаційній війні. Культурні та мистецькі студії ХХІ століття: науково-практичне партнерство : матеріали ІV Всеукр. наук.-практ. конф. / М-во культ. України та інформ. політики ; Нац. акад. кер. кадрів культ. і мистец. (Київ, 09 листопада 2023 р.). Київ, 2023. С. 255 URL: https://nakkkim.edu.ua/images/Instytuty/Akademiia/Vydannia/konferentsii/Tezy_09_11_2023_-2.pdf#page=255

Основна література:

1. Гринчак А. А. Протидія расизму, ксенофобії та екстремізму : навч. посіб. Харків : Лисенко І. Б., 2018. 246 с.
2. Данильченко Ю. Б. Тероризм: феномен, детермінація, протидія : [монографія]. Харків : Золота миля, 2018. 478 с.
3. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : АртЕк, 2018. 445 с.
4. Інформаційна безпека : навч. посіб. / за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Вид-во Львів. політехніки, 2019. 573 с.
5. Копієвська О. Р., Веденєєв Д. В. Hybrid threats as an object of educational practices in the cultural and artistic sphere of Ukraine (based on the experience of the Erasmus + project "Academic Counteraction to Hybrid Threats - #WARN" 610133-EPP-1-2019-1-FI-EPPKA2-SBHE-JP"). *Вісник Національної академії керівних кадрів культури і мистецтв*. Київ, 2021. 2. 3 – 11.
6. Петрик В. М., Присяжнюк М. М., Компанцева Л. Ф. та ін. Сугестивні технології маніпулятивного впливу: підручник. Київ, 2011. 248 с. URL: https://mil.univ.kiev.ua/files/29_965691167.pdf

7. Почепцов, Г. Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття. Київ : Києво-Могилянська академія, 2017. 257 с.
8. Світова гібридна війна: український фронт. За ред. Горбуліна В. П. Київ : Інститут стратегічних досліджень, 2017. 400 с.
9. Giannopoulos, G., Smith, H., Theocharidou, M. (Eds.) (2020). The Landscape of Hybrid Threats: A Conceptual Model Public Version <https://euhybnet.eu/wp-content/uploads/2021/06/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf>
10. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G. (2023). *Hybrid threats: a comprehensive resilience ecosystem – Executive summary*, Publications Office of the European Union, Luxembourg, doi:10.2760/113791, JRC129019
11. Kaldor, M., Human Security: Practical Possibilities. *LSE Public Policy Review*. 2020. 1(2), P. 7. DOI: <http://doi.org/10.31389/lseppr.15>

Допоміжна література:

12. Arcos R. & Palacios J.-M. (2018). The impact of intelligence on decision-making: the EU and the Arab Spring, *Intelligence and National Security*, 33:5, 737-754, DOI: 10.1080/02684527.2018.1434449
13. Arcos R. & Palacios J.-M. (2020) EU INTCEN: a transnational European culture of intelligence analysis?, *Intelligence and National Security*, 35:1, 72-94, DOI:10.1080/02684527.2019.1649912
14. Appelbaum E. Extremism as a strategic tool in conflicts / E. Appelbaum // *Journal of Economic Behavior & Organization*, 2008. № 68. P. 352–364.
15. Bartoli A Addressing extremism [Електронний ресурс] / Andrea Bartoli, Peter Coleman. URL: <http://www.tc.columbia.edu/icccr/index.asp>
16. Cristina Ivan, Irena Chiru & Rubén Arcos (2021) A whole of society intelligence approach: critical reassessment of the tools and means used to counter information warfare in the digital age, *Intelligence and National Security*, 36:4, 495-511, DOI: 10.1080/02684527.2021.1893072
17. European Commission (2020). Communication on tackling online disinformation. URL: <https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation>.
18. Falk, B.J. (2020) Strategic citizens: Civil society as a battlespace in the era of hybrid threats. *Hybrid CoE Strategic Analysis No 25*. – 8 p. - https://www.hybridcoe.fi/wp-content/uploads/2020/11/SA25_Strategic-Citizen.pdf
19. Joint Communication to the European Parliament and the Council «Joint Framework on countering hybrid threats the European Union response» (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018>
20. Martti J. Kari (2019). Russian Strategic Culture in Cyberspace. *Theory of Strategic Culture – a tool to Explain Russia’s Cyber Threat Perception and Response to Cyber Threats*. University of Jyväskylä. 211 p.
21. Mölder H., Sazonov V., Chochia A., Kerikmäe T. (Eds.) (2021). *The Russian Federation in Global Knowledge Warfare Influence Operations in Europe and Its Neighbourhood*. Springer. 424 p. DOI: 10.1007/978-3-030-73955-3
22. Schmid Johann (2019). Hybrid warfare on the Ukrainian battlefield: developing theory based on empirical evidence. *Journal on Baltic Security*, URL: <https://sciendo.com/article/10.2478/jobs-2019-0001>
23. Simonsen C. *Terrorism: the past, the players, and the future*. New Jersey: Pearson «Prentice Hall», 2004. 446 p.
24. Wigell Mikael (2019) Hybrid interference as a wedge strategy: a theory of external

interference in liberal democracy. *International Affairs*, Volume 95, Issue 2, March 2019, Pages 255–275, <https://doi.org/10.1093/ia/iiz018>

Інформаційні ресурси в Інтернеті:

25. Міністерство культури та інформаційної політики України [сайт]. URL: <https://mkip.gov.ua/>
26. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) [official site]. URL: <https://www.hybridcoe.fi/>
27. WARN «Academic Response to Hybrid Threats» [site of the project]. URL: <https://warn-erasmus.eu/ua/>