

# ГІБРИДНІ ЗАГРОЗИ ТА КОМПЛЕКСНА БЕЗПЕКА

## Силабус

№	Назва поля	Контент, коментарі
1.	Рівень вищої освіти	Другий (магістерський)
2.	Спеціальність	14.03 Середня освіта (Історія)
3.	Тип і назва освітньої програми	Освітньо-професійна програма – Середня освіта (Історія). Психологія
4.	Статус дисципліни	Основна
5.	Мова викладання	Українська
6.	Кількість ЄКТС кредитів	5
7.	Структура дисципліни (розподіл за видами та годинами навчання)	Лекції – 24 годин. Семинарські заняття – 20 годин Практичні заняття – 10 годин Самостійна робота – 96 годин
8.	Форма підсумкового контролю	Іспит
9.	Графік (терміни) вивчення дисципліни	I-й курс, I-й семестр
10.	Цілі навчання за дисципліною	<b>Мета дисципліни:</b> надати знання та навички, необхідні для розуміння, аналізу та реагування на гібридні загрози в професійній діяльності та громадському житті;
11.	Результати навчання	<p>Реалізовувати у власній професійній діяльності ефективні психолого-педагогічні стратегії існування людини в суспільстві в умовах сучасного глобалізованого соціокультурного середовища та гібридних загроз;</p> <p>Розуміти комплексну природу, складність, логіку і закономірності гібридних загроз, критично оцінювати соціально-політичні, економічні, культурні події та явища;</p> <p>Виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії;</p> <p>Виважено діяти у новій ситуації, реалізовувати ефективні стратегії існування людини в суспільстві в умовах сучасного глобалізованого соціокультурного середовища та гібридних загроз;</p> <p>Організовувати та реалізовувати просвітницьку та освітню діяльність для різних категорій населення з у сфері педагогіки, психології, історії, зокрема з питань виявлення та протидії гібридним загрозам.</p>
12.	Анотація (зміст) дисципліни	<b>Модуль 1.</b> Асиметрія, гібридні загрози та безпека. Новий безпековий ландшафт та прийняття рішень. Історія зародження і розвитку гібридних загроз. Визначення гібридних загроз. Суттєві ознаки (синхронізація, нелінійність,

		<p>неідентифікованість, «невідомі невідомі», міждисциплінарність, асиметричність та ін. ). Поняття PMESII –спектр. Поняття «4+1+AL» (земля, повітря, море, космос+ кібер)</p> <p><b>Модуль 2.</b> Концептуальна модель гібридних загроз. Підгрунття. Елементи та структура моделі. Державні та недержавні актори (гравці), їх використання у гібридних впливах.</p> <p><b>Модуль 3.</b> Домени (сфери) гібридних загроз. Розробка списку змінних показників, останнє розширення і визначення 13 доменів шкідливих дій: -інформація, - кібер напрямок, - космос, економіка, - військовий/оборонний, - культурний, -соціальний/, громадський, - адміністрація, - право, - розвідка, - дипломатія, - політичний, - інфраструктурний.</p> <p><b>Модуль 4.</b> Інструменти гібридних загроз. Інфраструктурні інструменти (фізичні операції проти об'єктів інфраструктури, інфраструктурні залежності та ін.). Кіберінструменти (кібершпигунство, кібероперації, заглушення, спуфінг GNSS та ін.). Економічні інструменти (економічні залежності, прямі закордонні інвестиції, промислове шпигунство, підрив національної економіки, використання економічних труднощів та ін.). Збройні/парамілітарні інструменти ( порушення територіальної цілісності, поширення зброї, операції збройних сил, військові навчання, воєнізовані (проксі) організації). Соціально-культурні інструменти (діаспори, культурні групи, релігія, міграція, система цінностей, соціокультурні розколи, вплив на освітні програми та наукові кола тощо). Інструменти в публічному управлінні (корупція, управління надзвичайними ситуаціями, експлуатація порогових значень, невіднесення тощо). Правові інструменти (залучення юридичних норм, процесів, установ та аргументів, законодавча невизначеність та ін.). Розвідувально-дипломатичні інструменти (підпільні організації, розвідувальні дії, проникнення, санкції, бойкоти посольства). Інформаційно-аналітичні інструменти (нарративи, інструменталізація історії, дискредитація, плутанина, підтримка акторів, примус політиків/уряду). Медіа-інструменти (медіа-контроль і втручання, дезінформаційні кампанії, пропаганда та ін).</p> <p><b>Модуль 5.</b> Динаміка гібридних загроз. Роль різних видів діяльності в ландшафті гібридних загроз. Фази гібридних загроз: підготовка,</p>
--	--	---

		<p>дестабілізація та примус. Гібридні активності: втручання, вплив, операції/кампанії та війна.</p> <p>Модуль 6. Основи захисту. Чотири хвили стримування та базові підходи до протидії гібридним загрозам ( інтегрований підхід, самооцінка, аналіз, захист/оборона). Комплексна концепція безпеки (на прикладі фінської моделі): готовність суспільства, багаторівнева модель антикризового менеджменту (загальнодержавний + місцевий рівні), структура державної системи протидії гібридним загрозам, принципи координації зусиль.</p>
13.	Система оцінювання	<p>Оцінювання знань студентів з навчальної дисципліни «Гібридні загрози та комплексна безпека» здійснюється шляхом проведення контрольних заходів, які включають поточний, підсумковий модульний, підсумковий семестровий контроль. Рівень навчальних досягнень здобувачів оцінюється за 100-бальною шкалою. Загальна сума балів складається з балів за контрольні точки та контрольні роботи залікового модулю, які проводяться на практичних заняттях, а також балів, які отримує здобувач на екзамені.</p>
14.	Якість освітнього процесу	<p>Політика курсу заснована на політиці Горлівського інституту іноземних мов Донбаського державного педагогічного університету, який є вільним і автономним центром освіти, що покликаний давати адекватні відповіді на виклики сучасності, плекати й оберігати духовну свободу людини, що робить її спроможною діяти згідно з власним сумлінням; її громадянську свободу, яка є основою формування суспільно відповідальної особистості, академічну свободу та академічну добросовісність, що є головними рушійними силами наукового поступу. Внутрішня атмосфера інституту будується на засадах відкритості, прозорості, гостинності, повазі до особистості.</p> <p>Результатом підготовки до заняття повинно бути змістовне володіння здобувачем вищої освіти матеріалом теми, якій присвячено відповідне заняття, а саме: підтвердження теоретичного матеріалу прикладами з історичних джерел, знання основних дефініцій, уміння аргументовано викласти певний матеріал, підготувати презентацію власних навчальних пошуків, коментувати відповіді інших здобувачів, доповнювати їх, знаходити помилки (неточності, недоліки) та надавати правильну відповідь, працювати в команді.</p>

		<p>Відповідь здобувача повинна демонструвати ознаки самостійності виконання поставлених завдань, відсутність ознак повторюваності та плагіату.</p> <p>Здобувач вищої освіти повинен дотримуватися навчальної етики, поважно ставитися до учасників процесу навчання, бути зваженим, уважним та дотримуватися дисципліни й часових (строкових) параметрів навчального процесу.</p>
15.	Сторінка курсу на платформі Moodle	<p><a href="http://dl.forlan.org.ua/login/index.php">http://dl.forlan.org.ua/login/index.php</a> - для входу в систему отримайте особистий пароль (деканат або технічна служба підтримки – <a href="mailto:support@forlan.org.ua">support@forlan.org.ua</a>)</p>
16.	Література	<p>Web-site of Hybrid CoE <a href="https://www.hybridcoe.fi/">https://www.hybridcoe.fi/</a></p> <p>Glossary of hybrid threats <a href="https://warn-erasmus.eu/ua/glossary/">https://warn-erasmus.eu/ua/glossary/</a></p> <p>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</p> <p>MCDC(a) (Multinational Capability Development Campaign project, 2019). Countering hybrid warfare project: Countering hybrid warfare. 93 p.</p> <p>Sweijjs, T., &amp; Zilincik, S. (2019). Cross Domain Deterrence and Hybrid Conflict. Hague Centre for Strategic Studies. 38p.</p>
17.	Матеріально-технічне, лабораторне, програмне забезпечення дисципліни	<p>Спеціалізована навчальна лабораторія дослідження гібридних загроз – учасник міжгалузевого середовища з протидії гібридним загрозам WARN (аудиторія 402 навчального корпусу). В 2021 році лабораторія отримала потужне комп'ютерне обладнання на загальну суму майже 894 тис. грн., профінансоване грантом проекту Еразмус+ «Академічна протидія гібридним загрозам – WARN» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP)</p>
18.	Кафедра	<p>Вітчизняної та зарубіжної історії, <a href="http://forlan.org.ua/?page_id=3">http://forlan.org.ua/?page_id=3</a></p>
19.	Викладач(и) – розробник(и) силябусу	<p>Докашенко Г.П., д. іст.н., проф. <a href="mailto:g.dokashenko@forlan.org.ua">g.dokashenko@forlan.org.ua</a> Докашенко В.М., д. іст.н., проф. <a href="mailto:v.dokashenko@forlan.org.ua">v.dokashenko@forlan.org.ua</a></p>