Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет інформаційно-аналітичних технологій та менеджменту
(повна назва)
Кафедра економічної кібернетики та управління економічною безпекою
(повна назва)

ЗАТВЕРДЖУЮ
Декан факультету ІТМ

В.Дорош Володимир ДОРОШЕНКО
(підпис, ім'я, прізвище)
«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Гібридні загрози та комплексна безпека
(назва навчальної дисципліни)
рівень вищої освіти другий (магістерський)
(бакалаврський, магістерський, освітньо-науковий)
спеціальність D3 Менеджмент
(код і повна назва спеціальності)
освітньо-професійна програма
(професійна або наукова)
Менеджмент
(повна назва програми)

Харків – 2025 р.

Розробник(и): С.В. Гришко, професор кафедри економічної кібернетики та управління економічною безпекою, к.е.н., доцент_____
(ініціали, прізвище, посада, науковий ступінь, вчене звання)

Робочу програму схвалено на засіданні кафедри економічної кібернетики та управління економічною безпекою_____

Протокол від «29» серпня 2025 р. № 1

Завідувач кафедри _____ Тетяна ПОЛОЗОВА
(підпис) (ім'я, прізвище)

Гарант освітньо-професійної програми _____ Світлана ГРИШКО
(підпис) (ім'я, прізвище)

Схвалено методичною комісією факультету ___ІТМ_____

Протокол від «29» серпня 2025 р. № 1

Голова методичної комісії _____ Аліна ШАФРОНЕНКО__
(підпис) (ім'я, прізвище)

1 ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Характеристика навчальної дисципліни*</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС* – 4</td><td colspan="2">Вибіркова дисципліна професійної та практичної підготовки за освітньою програмою «Менеджмент»</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>1-й</td><td>1-й</td></tr>
<tr><td>Індивідуальних завдань* :
навчальним планом не передбачено</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="15">Загальна кількість годин* – 120

Мова навчання – українська</td><td>2-й</td><td>2-й</td></tr>
<tr><td colspan="2">Кількість годин</td></tr>
<tr><td>120</td><td>120</td></tr>
<tr><td colspan="2">Навчальні заняття:
1) лекції, год.</td></tr>
<tr><td>22</td><td>8</td></tr>
<tr><td colspan="2">2) практичні, год.</td></tr>
<tr><td>18</td><td>8</td></tr>
<tr><td colspan="2">3) лабораторні, год.</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">4) консультації, год.</td></tr>
<tr><td>8</td><td>14</td></tr>
<tr><td colspan="2">Самостійна робота, год.</td></tr>
<tr><td>72</td><td>90</td></tr>
<tr><td colspan="2">в тому числі: КР, год.</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Вид контролю:
залік</td></tr>
</table>

Примітка.

* Відомості з навчального плану.

** Структурна одиниця дисципліни (складається із змістових модулів). Рекомендована кількість модулів дорівнює кількості контрольних точок.

2. МЕТА ДИСЦИПЛІНИ ТА ОЧІКУВАНІ РЕЗУЛЬТАТИ ЇЇ ВИВЧЕННЯ

2.1 Мета вивчення дисципліни

Метою вивчення дисципліни є формування у здобувачів системного розуміння природи гібридних загроз, їхніх доменів та інструментів, а також вироблення навичок оцінювання ризиків і розроблення комплексних підходів до забезпечення безпеки та підвищення стійкості суспільних, державних і корпоративних систем в умовах динамічного безпекового середовища.

«Гібридні загрози та комплексна безпека» – це новаторська дисципліна, розроблена в рамках проекту Еразмус+ «Академічна протидія гібридним загрозам» (WARN) 610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP[1].

Завданням дисципліни є розкрити сутність асиметрії та гібридних загроз як багатовимірного феномену сучасної безпеки; ознайомити здобувачів із концептуальними моделями гібридних загроз та методами їх аналізу; вивчити основні домени (сфери) застосування та інструменти гібридних впливів; проаналізувати динаміку розвитку гібридних загроз у глобальному та регіональному вимірах; сформувати розуміння стійкості як ключової властивості системи безпеки; надати базові знання щодо організації захисту держави, суспільства, бізнесу та особи в умовах гібридних загроз; розвинути у здобувачів здатність критично оцінювати інформацію, виявляти ризики та пропонувати комплексні безпекові рішення.

2.2 Результати навчання

За результатом вивчення дисципліни здобувачі вищої освіти **повинні знати**:

- сутність та особливості асиметрії і гібридних загроз у сучасному безпековому середовищі;
- концептуальні підходи та моделі аналізу гібридних загроз;
- основні домени (військовий, політичний, економічний, інформаційний, кібернетичний, соціокультурний тощо) та інструменти гібридних впливів;
- закономірності розвитку й динаміку гібридних загроз на національному та міжнародному рівнях;
- поняття «стійкість» як системну характеристику безпеки та фактори, що її визначають;
- принципи і методи організації комплексного захисту в умовах гібридних загроз;
- основи державної, суспільної та корпоративної політики у сфері протидії гібридним загрозам.

---

[1] Дисклаймер (застереження): 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.

За результатом вивчення дисципліни здобувачі вищої освіти **повинні вміти**:

- ідентифікувати та класифікувати прояви гібридних загроз у різних доменах;
- аналізувати інформацію для виявлення ознак гібридних впливів та оцінки їхнього потенційного впливу;
- використовувати концептуальні моделі для прогнозування розвитку гібридних загроз;
- оцінювати рівень стійкості системи та визначати її вразливості;
- розробляти пропозиції щодо заходів протидії гібридним загрозам та підвищення безпеки;
- застосовувати комплексний підхід до планування захисних і превентивних заходів;
- аргументовано обґрунтовувати управлінські рішення у сфері безпеки з урахуванням багатофакторного впливу гібридних загроз.

Перелік сформованих компетентностей (відповідно до освітньо-професійної програми):

- загальні компетентності (ЗК):

ЗК2. Здатність до спілкування з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

ЗК5. Здатність діяти на основі етичних міркувань (мотивів).

ЗК7. Здатність до абстрактного мислення, аналізу та синтезу;

- спеціальні (фахові, предметні) компетентності (СК):

СК2. Здатність встановлювати цінності, бачення, місію, цілі та критерії, за якими організація визначає подальші напрями розвитку, розробляти і реалізовувати відповідні стратегії та плани.

СК9. Здатність аналізувати й структурувати проблеми організації, приймати ефективні управлінські рішення та забезпечувати їх реалізацію.

СК11. Здатність соціально відповідально адаптувати робочі процеси та особистий простір до складних та непередбачуваних ситуацій, спричинених гібридними загрозами.

Програмні результати навчання (РН) (відповідно до освітньо-професійної програми):

РН1. Критично осмислювати, вибирати та використовувати необхідний науковий, методичний і аналітичний інструментарій для управління в непередбачуваних умовах.

РН2. Ідентифікувати проблеми в організації та обґрунтовувати методи їх вирішення.

РН6. Мати навички прийняття, обґрунтування та забезпечення реалізації управлінських рішень в непередбачуваних умовах, враховуючи вимоги чинного законодавства, етичні міркування та соціальну відповідальність.

РН14. Виявляти, ідентифікувати, класифікувати гібридні загрози та ефективно на них реагувати в міжгалузевій взаємодії на основі пріоритетів сталого розвитку.

2.3 Передумови вивчення дисципліни

Передумовою вивчення дисципліни є раніше здобуті компетентності та результати навчання, що перевіряються під час єдиного фахового вступного випробування зі спеціальності на основі Програми предметного тесту з управління та адміністрування єдиного фахового вступного випробування для вступу на навчання для здобуття ступеня магістра, затвердженого Наказом Міністерства освіти і науки України від 11.02.2022 р. № 157 «Про затвердження Програми предметного тесту з управління та адміністрування єдиного фахового вступного випробування». Загальна структура предметного тесту передбачає три основні розділи: Менеджмент, Маркетинг, Підприємництво.

3 ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль І. Сутність гібридних загроз

Тема 1. Асиметрія, гібридні загрози та безпека

Новий безпековий ландшафт та прийняття рішень, прийняття рішень в демократичних та недемократичних суспільствах. Розмиття дихотомій.

Гібридні загрози: історія поняття.

Визначення гібридних загроз та їх суттєві ознаки (синхронізація, нелінійність, неідентифікованість, "невідомі невідомі", "злісні проблеми", міждисциплінарність, асиметричність).

PMESII-спектр (знайомство з доменами), концепція "4+1+AI".

Тема 2. Концептуальна модель гібридних загроз

Підґрунтя, елементи (гравці, домени, інструменти та фази) та структура концептуальної моделі гібридних загроз.

Державні актори (гравці) гібридних загроз. Гібридні впливи як сила слабких. Ключові характеристики держав, що вдаються до гібридних загроз, їх відмінність від інших країн. Російське стратегічне мислення. Стратегічна культура Китаю.

Недержавні гравці гібридних загроз, їх таксономія та використання у гібридних впливах.

Тема 3. Домени (сфери) та інструменти гібридних загроз

Основні підходи до визначення доменів гібридних загроз (критичні функції та вразливості).

Визначення, вразливості та приклади по конкретним доменам: інфраструктурні домени, кібер- домени, домени космічної діяльності, економічні домени, військові / оборонні / парамілітарні домени, культурні домени, соціальні / громадські домени, домени державного управління, правові домени, домени розвідувальної діяльності, дипломатичні домени, політичні домени, інформаційні домени.

Система інструментів діяльності гібридних загроз. Особливості та приклади використання окремих груп інструментів: інфраструктурні інструменти, кіберінструменти та електронні операції, економічні інструменти, збройні / парамілітарні інструменти, соціально-культурні інструменти, інструменти в державному управлінні, юридичні інструменти, розвідувально-дипломатичні інструменти, інформаційно-аналітичні інструменти, медіа-інструменти.

Змістовий модуль ІІ. Протидія гібридним загрозам

Тема 4. Динаміка гібридних загроз

Роль різних видів діяльності в ландшафті гібридних загроз.

Основні фази гібридних впливів: підготовка, дестабілізація та примус.

Основні види гібридних впливів (активностей): втручання, вплив, операції / кампанії та війна.

Тема 5. Стійкість як ключова безпекова властивість

Концепція стійкості як основа для формування захисту в умовах гібридних загроз. Стійкість як властивість. Стійкість соціально-економічних систем та індивідуальна стійкість.

Стійкість в контексті гібридних загроз. Комплексна модель екосистеми стійкості (CORE model). Розгляд складових CORE-моделі з точки зору стійкості: 7 основ демократичних систем; 13 доменів гібридних загроз; 3 простори екосистеми; шари екосистемі – від локальних до міжнародних рівнів. Практичне застосування екосистеми за принципом "дартса": відображення впливу гібридних загроз.

Створення стійкості до гібридних загроз на основі CORE-моделі: основні підходи.

Тема 6. Основи захисту в умовах гібридних загроз

Історія захисту від гібридних впливів ("чотири хвилі 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 кризового менеджменту (державний + регіональний + місцевий рівні), структура державної системи протидії гібридним загрозам, принципи координації зусиль на різних рівнях та доменах.

Самооцінка: критичні функції - параметри, пороги та індикатори.

Протидія: концептуальна модель протидії гібридним загрозам – виявлення, стримування, реагування; роль обізнаності населення в стійкості суспільства; державні та волонтерські проєкти (EU StratCom, StopFake…)

Виявлення загроз та їх розпізнавання: моніторинг та відкриття.

Стримування: принципи ‘три Cs’ стримування та інші; крос-доменне стримування – атрибуція, визнання, пропорційність, сигналізація; види стримування – спеціальне, пунктуаційне, кумулятивне; стратегії стримування – заперечення, покарання; індивідуальна адаптація до гібридів супротивника.

Реагування: концептуальна модель – стратегічні цілі та пороги відповіді, шляхи та засоби, ключові фактори; реагування на гібридні атаки за допомогою важелів PMESII.

Принципи побудови механізмів для захисту від гібридних загроз: основні підходи; створення механізму виявлення - моніторингові системи та механізми виявлення і роботи з аномаліями та слабкими сигналами; створення механізмів стримування– концепції, органи із повноваженнями та ресурсним забезпеченням; алгоритми дій для непередбачуваних ситуацій; заходи для забезпечення обізнаності; посилення зовнішньої взаємодії; ‘top-down’ та ‘bottom-up’ заходи: процеси, механізми, люди та навички реалізації стратегії.

4 СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	усього	у тому числі				усього	у тому числі			
		лк	пз	конс	с.р.		лк	пз	конс	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Змістовий модуль І. Сутність гібридних загроз										
Тема 1. Асиметрія, гібридні загрози та безпека	16	2	2		12	19	1	1	2	15
Тема 2. Концептуальна модель гібридних загроз	22	4	4	2	12	22	2	2	3	15
Тема3. Домени (сфери)та інструменти гібридних загроз	20	4	2	2	12	19	1	1	2	15
Разом за змістовим модулем І	**58**	**10**	**8**	**4**	**36**	**60**	**4**	**4**	**7**	**45**
Змістовий модуль ІІ. Протидія гібридним загрозам										
Тема 4. Динаміка гібридних загроз	16	2	2		12	19	1	1	2	15
Тема 5. Стійкість як ключова безпекова властивість	22	4	4	2	12	19	1	1	2	15
Тема 6. Основи захисту в умовах гібридних загроз	24	6	4	2	12	22	2	2	3	15
Разом за змістовим модулем ІІ	**62**	**12**	**10**	**4**	**36**	**60**	**4**	**4**	**7**	**45**
Усього за семестр	**120**	**22**	**18**	**8**	**72**	**120**	**8**	**8**	**14**	**90**

5 ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№	Назва теми	Кількість годин	
		денна	заочна
1	Тема 1. Асиметрія, гібридні загрози та безпека	2	1
2	Тема 2. Концептуальна модель гібридних загроз	4	2
3	Тема3. Домени (сфери)та інструменти гібридних загроз	2	1
4	Тема 4. Динаміка гібридних загроз	2	1
5	Тема 5. Стійкість як ключова безпекова властивість	4	1
6	Тема 6. Основи захисту в умовах гібридних загроз	4	2
	Усього	**18**	**8**

6 ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

Лабораторні роботи не передбачені навчальним планом.

7 САМОСТІЙНА РОБОТА

№	Вид самостійної роботи	Кількість годин	
		денна	заочна
1	Вивчення теоретичного матеріалу з використанням конспектів і навчальної літератури та англомовних першоджерел	12	15
2	Підготовка до практичних занять	20	30
3	Підготовка до виконання самостійних досліджень з пошуком інформації в англомовних джерелах	40	45
	Усього	**72**	**90**

8 ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуальні завдання не передбачені навчальним планом.

9 МЕТОДИ НАВЧАННЯ ТА ЗАСОБИ ОЦІНЮВАННЯ

Вивчення дисципліни «Гібридні загрози та комплексна безпека» здійснюється зі застосуванням різних методів.

Словесні методи навчання містять *лекції*, які розкривають сутність наукових понять, явищ та процесів, які пов'язані загальною темою; *пояснення*, за допомогою яких розкривається сутність закону або процесу з використанням попереднього досвіду здобувачів; *розповіді* з метою спонукання здобувачів до створення в уяві певного образу; евристичних та репродуктивних *бесід*, які передбачають приведення попередніх знань до усвідомлення нових явищ та понять.

Наочні методи навчання, які передбачають *демонстрацію* (показ процесів у динаміці), ілюстрацію (схеми, графіки) та *спостереження* (сприймання процесів без втручання у ці процеси).

Практичні методи навчання сприяють формуванню вмінь і навичок, логічному завершенню ланки пізнавального процесу стосовно конкретної теми або розділу. Вони містять: *семінарські заняття*, спрямовані на використання набутих знань у розв'язанні практичних завдань; також виконання *письмових вправ* з метою цілеспрямованого повторення здобувачами окремих дій задля формування умінь та навичок за дисципліною.

Особливістю курсу є використання **методики проактивного навчання**, розробленої в межах проєкту Erasmus+ WARN (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP). Вона спрямована на формування у здобувачів здатності діяти ефективно в умовах гібридних впливів, інформаційних перевантажень та кризових ситуацій, що відповідає сучасним викликам управління безпекою організацій.

10 МЕТОДИ КОНТРОЛЮ ТА РЕЙТИНГОВА ОЦІНКА ЗА ДИСЦИПЛІНОЮ

10.1 Розподіл балів, які отримують здобувачі (кількісні критерії оцінювання).

Під час освітнього процесу застосовуються контрольні заходи поточного та підсумкового контролю.

Поточний контроль здійснюється під час проведення різних видів навчальних занять і має на меті перевірку рівня знань здобувачів вищої освіти з відповідної дисципліни. Проведення поточного контролю здійснюється під час навчальних занять, а оцінювання успішності здобувачів вищої освіти визначається робочою програмою навчальної дисципліни (РПНД). Види поточного контролю визначаються даною РПНД.

Підсумковий контроль – контрольні заходи, що передбачають встановлення відповідності (вимірювання, оцінювання) здобутих особою результатів навчання вимогам освітньої програми у частині відповідного освітнього компонента.

Підсумковий контроль з даної дисципліни проводиться у формі заліку.

Контрольний захід у формі заліку полягає в оцінюванні засвоєння здобувачем вищої освіти навчального матеріалу на підставі результатів поточного контролю та передбачає підведення підсумків протягом першого тижня екзаменаційної сесії за розкладом.

Присутність здобувача вищої освіти на контрольному заході у формі заліку не є обов'язковою.

Здобувач вищої освіти отримує позитивну оцінку на заліку за умови виконання всіх видів робіт, передбачених РПНД, та за наявності оцінок за кожен вид робіт, що не менше відповідного встановленого мінімального бала.

Підсумковий контроль з дисципліни у формі заліку оцінюється кількістю балів, отриманих здобувачем вищої освіти за виконання всіх видів поточного контролю протягом семестру за 100-бальною шкалою:

$$О_д = 0{,}6 \cdot О_{сем} + Р \cdot О_{сем},$$

де $О_д$ – підсумкова оцінка з дисципліни в семестрі;

$О_{сем}$ – сумарна кількість балів, отриманих здобувачем вищої освіти протягом семестру (від 1 до 100 балів), що визначається за формулою:

$$О_{сем} = \sum О_i,$$

де $О_i$ – кількість балів з і-го контрольного заходу поточного контролю дисципліни;

Р – ознака виконання всіх видів робіт: Р=0,4, якщо виконані всі види робіт з позитивною оцінкою, Р=0 – в іншому випадку (за відсутності позитивної оцінки хоча б з одного поточного контрольного заходу з дисципліни, передбаченого РПНД).

Оцінка за семестр ($О_{сем}$) з навчальної дисципліни визначається відповідно до таблиці 10.1.

Таблиця 10.1 – Розподіл балів, що отримує здобувач вищої освіти протягом семестру

Номер модуля	Вид заняття/контрольний захід	Оцінка *О*сем
1	ПЗ № 1	10
	ПЗ № 2	10
	ПЗ № 3	10
	ПЗ № 4	15
	Контрольна точка 1	**45**
2	ПЗ № 5	10
	ПЗ № 6	10
	ПЗ № 7	10
	ПЗ № 8	10
	ПЗ № 9	15
	Контрольна точка 2	**55**

Отримані бали переводяться за національною шкалою та шкалою ЄКТС.

Для підсумкового контролю використовуються шкали оцінок, наведені у таблиці 10.2.

Таблиця 10.2 – Шкали оцінок для визнання успішності навчання здобувачів вищої освіти

Оцінка з дисципліни	Оцінка ЄКТС	Оцінка за національною шкалою	
		екзамен, курсовий проєкт (робота), практика	залік
96-100	A	5 (відмінно)	зараховано
90-95	B	5 (відмінно)	
75-89	C	4 (добре)	
66-74	D	3 (задовільно)	
60-65	E	3 (задовільно)	
35-59	FX	2 (незадовільно)	незараховано
1-34	F		

10.2 Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

1. Сутність та особливості асиметрії й гібридних загроз у сучасному безпековому середовищі.

2. Концептуальні підходи, моделі та основні домени застосування гібридних загроз і їх інструменти.

3. Закономірності розвитку та динаміку гібридних загроз на національному й міжнародному рівнях.

4. Поняття стійкості як ключової властивості безпеки та фактори, що її визначають.

5. Принципи організації комплексного захисту та засади державної, суспільної й корпоративної політики протидії гібридним загрозам.

Необхідний обсяг умінь для одержання позитивної оцінки:

1. Ідентифікувати та класифікувати прояви гібридних загроз у різних сферах.
2. Аналізувати інформацію та оцінювати потенційний вплив гібридних загроз.
3. Застосовувати концептуальні моделі для прогнозування розвитку гібридних загроз.
4. Оцінювати стійкість системи та виявляти її вразливості до гібридних впливів.
5. Розробляти та обґрунтовувати пропозиції щодо комплексних заходів протидії та безпеки соціально-економічних систем в умовах гібридних загроз.
6. Аргументовано формулювати соціально-економічні рішення з урахуванням протидії гібридним загрозам.

Критерії оцінювання роботи здобувача вищої освіти протягом семестру.

Задовільно, E (60-65): виставляється здобувачу, що виявив знання основного навчального матеріалу в мінімальному обсязі, необхідному для подальшого навчання та майбутньої професійної діяльності; в основному виконував завдання, передбачені програмою; ознайомився з основною літературою, рекомендованою програмою; припустив помилки у відповіді на запитання при співбесідах, тестуванні та при виконанні завдань тощо, які він може усунути лише під керівництвом та за допомогою викладача.

Задовільно, D (66-74): заслуговує здобувач, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання й майбутньої роботи за спеціальністю, впорався з виконанням завдань, передбачених програмою; припустив значну кількість помилок або недоліків у відповіді на запитання при виконанні завдань тощо, принципові які може усунути самостійно.

Добре, C (75-89): заслуговує здобувач, який виявив повні знання навчально-програмного матеріалу при виконанні передбачених програмою завдань, але припустив ряд помітних помилок; засвоїв основну літературу, рекомендовану програмою; показав систематичний характер знань з дисципліни; здатний до їх самостійного використання та поповнення в процесі подальшої навчальної роботи і професійної діяльності.

Відмінно, B (90-95): виставляється здобувачу, який виявив систематичні та глибокі знання навчального матеріалу з даної дисципліни вище середнього рівня. Він продемонстрував уміння вільно виконувати завдання, передбачені програмою; засвоїв літературу, рекомендовану програмою; засвоїв взаємозв'язок основних понять дисципліни та їх значення для подальшої професійної діяльності.

Відмінно, A (96-100): заслуговує здобувач, який виявив всебічні систематичні та глибокі знання навчально-програмного матеріалу, вміння вільно виконувати завдання, що передбачені програмою, засвоїв основну та додаткову літературу, яка рекомендована програмою; проявив видатні творчі здібності в розумінні, в логічному, чіткому, стислому та ясному трактуванні навчально-програмного матеріалу; засвоїв основні поняття дисципліни, їх значення для подальшої професійної діяльності.

11 МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ТА РЕКОМЕНДОВАНАЛІТЕРАТУРА

11.1 Базова література

1. Гібридні загрози та комплексна безпека: навчальний посібник. Укл. Карпенко О.О., Осипова Є.Л. Київ: ТОВ «ТРОПЕА», 2024. 76 с. https://doi.org/10.32703/978-617-8268-30-5
2. 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
3. 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.
4. Monaghan S., Cullen P., Wegge N. MCDC (Multinational Capability Development Campaign project): Countering Hybrid Warfare Project: Countering Hybrid Warfare. 2019. 93 p. URL: https://assets.publishing.service.gov.uk/gov...
5. Глосарій з гібридних загроз / Erasmus + project WARN "Academic Response to Hybrid Threats". 2024. 203с. https://openarchive.nure.ua/entities/publication/c2051668-3a66-458a-97a2-7df51697b99e

11.2 Допоміжна література

6. EU Security Union Strategy: Connecting the Dots in a New Security Ecosystem. Brussels, 2020. URL: https://ec.europa.eu/transparency/regdoc/rep...
7. Kaikova, O., Terziyan, V., Tiihonen, T., Golovianko, M., Gryshko, S., & Titova, L. Hybrid Threats against Industry 4.0: Adversarial Training of Resilience. E3S Web of Conferences 353. EDP Sciences. 2022. 14 p. URL: https://jyx.jyu.fi/bitstream/handle/123456789/82376/kaikovaym.pdf
8. Pijpers B.M.J., Ducheine, P.A.L. Influence Operations in Cyberspace – How they Really Work. Amsterdam Center for International Law (No. 2020-31). Amsterdam Law School Research Paper (No. 2020-61). 24.09.2020. 28 p. URL: https://ssrn.com/abstract=3698642
9. Mazzucchi N. AI-based Technologies in Hybrid Conflict: The Future of Influence Operations. Hybrid CoE Working Paper. June 2022. Vol. 14. 20 p. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf
10. Бусол О. Ю. Феномен гібридних загроз національній безпеці. Юридична Україна. 2020. № 4. С. 6-15.
11. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика: монографія; Українська академія друкарства, Львівський державний університет внутрішніх справ. Львів: Растр-7, 2020. 383 с.

11.3 Методичні вказівки до різних видів занять

1. Комплекс навчально-методичного забезпечення навчальної дисципліни «Гібридні загрози та комплексна безпека»: спеціальність D3 Менеджмент, освітньо-професійна програма «Менеджмент», факультет Інформаційно-аналітичних технологій та менеджменту / Розроб. С.В. Гришко. Харків: ХНУРЕ, 2025. 163 с.

12 НФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ

1. Європейський центр з протидії гібридним загрозам Hybrid CoE https://www.hybridcoe.fi/
2. Глосарій гібридних загроз https://warn-erasmus.eu/ua/glossary/
3. Сайт проекту Еразмус+ «Академічна протидія гібридним загрозам» (WARN) https://warn-erasmus.eu/ua/
4. Національна бібліотека України імені В.І. Вернадського. URL: http://www.nbuv.gov.ua
5. Наукова бібліотека Харківського національного університету радіоелектроніки. URL: http://lib.nure.ua
6. Електронний архів відкритого доступу Харківського національного університету радіоелектроніки. Наукові праці викладачів кафедри економічної кібернетики та управління економічною безпекою URL: http://openarchive.nure.ua/handle/document/67
7. Сайт кафедри економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки. Робочі програми навчальних дисциплін. URL: https://eces.nure.ua/studentam/robochi-programi