



ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФРАСТРУКТУРИ ТА  
ТЕХНОЛОГІЙ  
ІНСТИТУТ УПРАВЛІННЯ, ТЕХНОЛОГІЙ ТА ПРАВА  
ФАКУЛЬТЕТ УПРАВЛІННЯ І ТЕХНОЛОГІЙ  
КАФЕДРА МЕНЕДЖМЕНТУ, ПУБЛІЧНОГО УПРАВЛІННЯ ТА  
АДМІНІСТРУВАННЯ




СИЛАБУС НАВЧАЛЬНОЇ  
ДИСЦИПЛІНИ

**Гібридні загрози та  
комплексна безпека**

Затверджено:

Протокол засідання кафедри  
менеджменту, публічного  
управління та адміністрування  
№ 1 від 29 серпня 2022 р.  
В.о. завідувача кафедри МПУА  
Т.Б. Семенчук

Викладач	КАРПЕНКО Оксана Олександрівна Доктор економічних наук, професор	
Посилання профіль викладача на сайті ДУІТ	<a href="#">КАРПЕНКО Оксана Олександрівна</a>	
E-mail	karpo_2004@ukr.net	
Факультет, Кафедра	Факультет Управління і технологій/ Кафедра менеджменту та публічного адміністрування м. Київ, вул. Івана Огієнка, 19, каб. 608 телефон: +38066-451-23-32	
Консультації	Кожна п'ятниця з 12.00 до 13.00 за <u>ZOOM посиланням</u>	
Офіційна назва освітньої програми	Управління та адміністрування	
Рівень вищої освіти	третій (освітньо-науковий)	
Галузь знань, спеціальність	07 «Управління та адміністрування» 073 «Менеджмент»	
Статус дисципліни (обов'язкова, вибіркова)	Цикл дисциплін професійної підготовки, вибіркова	
Курс/ Семестр викладання	2/4	
Обсяг дисципліни	5 кредитів ECTS / 150 загальна кількість годин	
Види та кількість аудиторних занять, денна/ заочна	Лекції – 20 годин/ 8 годин Практичні заняття – 24 годин/ 4 години	
Форма контролю	Залік	

Локація та матеріально-технічне забезпечення	Аудиторія згідно з розкладом. Мультимедійний проектор, мережа Internet.
Мова викладання	Українська
Мета вивчення дисципліни	Формування системи знань та вмінь, необхідних для виконання організаційних, аналітичних та консультаційних функцій щодо ідентифікації та протидії гібридним загрозам і забезпечення комплексної безпеки на національному й міжнародному рівні.
Інтегральна компетентність	ІК. Здатність продукувати нові ідеї, розв'язувати комплексні проблеми у галузі управління та адміністрування, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики, застосовувати новітні методології наукової та педагогічної діяльності, здійснювати власні наукові дослідження, результати яких мають наукову новизну, теоретичне та практичне значення.
Загальні компетентності	ЗК04. Здатність розв'язувати комплексні проблеми у сфері менеджменту на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності).
Спеціальні (фахові) компетентності	СК01. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у менеджменті і дотичних до нього міждисциплінарних напрямках.
Програмні результати навчання	РН01. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи. РН02. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми менеджменту державною та англійською мовами, кваліфіковано відображати результати досліджень у наукових публікаціях у провідних міжнародних наукових виданнях. РН04. Розробляти та реалізовувати наукові та прикладні проекти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику у галузі управління та адміністрування і розв'язувати значущі наукові та технологічні проблеми в менеджменті з дотриманням норм академічної етики і врахуванням соціальних, етичних, економічних, екологічних та правових аспектів.

### **ЧИМ ВАЖЛИВИЙ КУРС:**

Курс дає можливість розширити світогляд та професійні компетенції, посиливши обізнаність щодо ідентифікації, розпізнавання, протидії гібридним загроз і забезпечення комплексної безпеки.

Курс розроблено та впроваджено з метою виконання завдань міжнародного проєкту Erasmus + «Академічна протидія гібридним загрозам» (Academic Response to Hybrid Threat, WARN), який реалізується в межах Програми Європейського Союзу Еразмус+ за напрямом

**ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ**  
**МОДУЛЬ 1. ГІБРИДНІ ЗАГРОЗИ ТА КОМПЛЕКСНА БЕЗПЕКА**  
**ЗМІСТОВИЙ МОДУЛЬ 1. ГІБРИДНІ ЗАГРОЗИ ТА КОМПЛЕКСНА БЕЗПЕКА**

**Тема 1. Асиметрія, гібридні загрози (HTs) та безпека**

Новий безпековий ландшафт та прийняття рішень; гібридні загрози - історія, визначення, основні характеристики; спектр PMESII; "4 + 1 + AI".

**Тема 2. Концептуальна модель гібридних загроз**

Ландшафт гібридних загроз: передумови, елементи та структура моделі; державні та недержавні актори, їх використання у гібридному впливі.

**Тема 3. Домени (сфери) гібридних загроз**

Критичні функції та вразливості; інформаційна, кібернетична, космічна, економічна, військова/оборонна, культурна, соціальна/суспільна, державне управління, правова, розвідувальна, дипломатична, політична, інфраструктурна сфери.

**Тема 4. Інструменти гібридних загроз**

Система інструментів гібридного впливу; операції проти інфраструктури; кібершпигунство та кібероперації, електронні операції, економічні, військові/воєнізовані, соціокультурні, інструменти в державному управлінні, правові, розвідувально-дипломатичні, інформаційно-аналітичні, медіа-інструменти.

**Тема 5. Динаміка гібридних загроз**

Роль різних видів діяльності в ландшафті гібридних загроз; фази гібридних загроз, гібридні види діяльності.

**Тема 6. Основи захисту**

Історія питання та основні підходів до протидії гібридним загрозам; концепція комплексної безпеки (на прикладі фінської моделі); самооцінка; протидія; моніторинг та виявлення гібридних загроз; стримування; реагування; принципи побудови механізмів захисту від гібридних загроз.

**Практичні заняття** курсу передбачають виконання ситуаційних, тестових та інших завдань, опитування та дискусії за темами, короткі виступи та презентації з тематики дисципліни.

Тематика практичних занять:

Практична робота №1,2. Асиметрія, гібридні загрози (HTs) та безпека.

Практична робота №3,4. Концептуальна модель гібридних загроз.

Практична робота №5,6. Домени (сфери) гібридних загроз.

Практична робота №7,8. Інструменти гібридних загроз.

Практична робота №9,10. Динаміка гібридних загроз.

Практична робота №11,12. Основи захисту.

**Приклади практичних завдань:**

**Ситуаційне завдання:**

Перейти за посиланням на сайт [Hybrid CoE](#) та зробити аналіз будь-якої публікації, результати якого представити у вигляді доповіді з презентацією на практичному занятті.

**Приклад тестового завдання:**

Скоординована та синхронізована дія, яка свідомо спрямована на системні вразливості демократичних держав та інститутів за допомогою широкого спектру засобів називається:

- а) гібридна війна;
- б) гібридна загроза;
- в) гібридний конфлікт;

г) гібридний вплив.

Для стимулювання науково-дослідницького й творчого інтересу здобувачів вищої освіти і здобуття ними навичок наукової діяльності вони залучаються до виконання додаткових видів робіт в певних проєктах, ця діяльність враховується при підведенні підсумків роботи здобувачів вищої освіти у семестрі. Так, наприклад, здобувачам вищої освіти може бути запропоновано виконання рефератів за темами дисципліни «Гібридні загрози та комплексна безпека» у вигляді презентацій та захистити її на практичному занятті. Найкращі рекомендуються до виступу на науково-практичній конференції.

Орієнтована тематика:

1. Міжнародний досвід протидії гібридним загрозам.
2. Стан досліджень гібридних загроз.
3. Дезінформація та пропаганда як складові гібридної війни.
4. Гібридні загрози та національна стратегія.
5. Протидія гібридним загрозам та ведення гібридної війни як частина національної стратегії держави.
6. Захист критичної інфраструктури.
7. Вибудовування національної стійкості до гібридних загроз: заходи пом'якшення наслідків.
8. Ризики переростання гібридних загроз у військові конфлікти.
9. Розмивання цивільного та військового спектрів маніпулювання інформацією з боку сучасних гібридних технологій.
10. Стратегія НАТО щодо протидії гібридним загрозам.
11. Концептуальні підходи НАТО та ЄС до забезпечення стійкості держави і суспільства у сфері національної безпеки.
12. Шляхи пом'якшення та протидії нинішнім та майбутнім гібридним загрозам через нові технології, як от штучний інтелект.
13. Питання гібридних загроз і соціальної безпеки у програмі НАТО «Партнерство заради миру» і Консорціуму оборонних академій та дослідницьких інституцій НАТО.
14. Україна-НАТО: спільна невійськова співпраця у протидії гібридній війні.
15. Підходи до гібридних загроз в ЄС.
16. Головні напрямки протидії гібридним загрозам та підвищення стійкості країн-членів ЄС до такого роду викликів.
17. Законодавство ЄС щодо протидії гібридним загрозам.
18. Стратегічні комунікації ЄС у контексті протидії пропаганді кібернетичним атакам, втручанням у вибори, кампаніям дезінформації у соціальних медіа.
19. Моніторинг джерел фінансування антиєвропейської пропаганди.
20. Боротьба з інформаційними війнами, дезінформацією та радикалізацією.
21. Організації з питань стратегічних комунікацій та протидії гібридним загрозам.
22. Стратегія ЄС з протидії пропаганді.
23. Стратегічний порядок денний ЄС на 2019-2024 роки.
24. Регіональні тенденції розвитку гібридних загроз.
25. Посилення протидії гібридним загрозам у Польщі.
26. Балтійський фронт протидії гібридній агресії.
27. Інформаційна сфера – ключовий вимір гібридної війни.
28. Актуальні гібридні загрози безпеці України.
29. Система політичних сил України як чинник гібридної війни.
30. Інформаційна безпека.
31. Кіберпростір як поле війни.
32. Державні можливості безпеки України: сучасний стан

Індивідуальні види робіт можуть бути змінені та доповнені за ініціативою викладача або здобувача освіти (за погодженням із викладачем).

### ОЦІНЮВАННЯ

Форми поточного та підсумкового контролю	Поточний контроль – 100 балів
КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ	
Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру.	

#### **Відвідування лекцій:**

За відвідування кожної лекції нараховується 1 бал (до 10 балів).

#### **Практичні заняття:**

Оцінюються за активністю здобувачів освіти на заняттях, їх відповідями, доповідями та ступенем залученості у дискусії. Максимальна сума становить 7,5 балів за кожне заняття (до 90 балів).

#### **Самостійна робота**

Написання та захист реферату (тематика погоджується із викладачем курсу) у вигляді доповіді та/або презентації оцінюються до 10 балів.

Здобувач отримує підсумкову оцінку за результатами поточного контролю шляхом накопичення балів. Максимальна кількість балів, яку може отримати здобувач, становить 100.

Додаткові бали до поточного контролю здобувач освіти може отримати, пройшовши навчальний курс у вигляді неформальної освіти з отриманням сертифікату в межах предмету вивчення дисципліни та пройшовши процедуру визнання згідно [Положення про визнання результатів навчання, отриманих у неформальній освіті здобувачами вищої освіти ДУІТ](#).

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS			
Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	Відмінно («зараховано»)	A	«Відмінно» - теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконанні в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
82-89	Добре («зараховано»)	B	«Дуже добре» - теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконанні, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками
75-81		C	«Добре» - теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконанні, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками
64-74	Задовільно («зараховано»)	D	«Задовільно» - теоретичний зміст курсу освоєний не повністю, але прогалини не носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками

60-63		Е	«Достатньо» - теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального, робота, що задовольняє мінімум критеріїв оцінки
35-59	Незадовільно («не зараховано»)	FX	«Умовно незадовільно» теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота що потребує доробки
1-34		F	«Безумовно незадовільно» теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

### ІНФОРМАЦІЙНО- МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Методичне забезпечення:

1. Робоча програма навчальної дисципліни.
2. Силабус навчальної дисципліни.
3. Посилання на Google Classroom: [Гібридні загрози та комплексна безпека](#)

Електронні ресурси бібліотеки ДУІТ: <https://library.duit.in.ua>.

### СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

**Базова:**

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 URL: <https://publications.jrc.ec.europa.eu/repository/handle/JRC123305>
2. Європейський центр з протидії гібридним загрозам Hybrid CoE <https://www.hybridcoe.fi/>
3. Глосарій гібридних загроз <https://warn-erasmus.eu/ua/glossary/>
4. Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. - Swedish Defence University. ISBN 978-91-86137-73-1. URL: <https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf>
5. EU Security Union Strategy: connecting the dots in a new security ecosystem. URL: [file:///C:/Users/user/Downloads/EU\\_Security\\_Union\\_Strategy\\_\\_connecting\\_the\\_dots\\_in\\_a\\_new\\_security\\_ecosystem.pdf](file:///C:/Users/user/Downloads/EU_Security_Union_Strategy__connecting_the_dots_in_a_new_security_ecosystem.pdf)
6. JOINT STAFF WORKING DOCUMENT. Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. Brussels, 24.7.2020.SWD(2020) 153 final. URL: <https://ec.europa.eu/transparency/regdoc/rep/10102/2020/EN/SWD-2020-153-F1-EN-MAIN-PART-1.PDF>
7. Business community and hybrid threats: Report of Pasi Eronen Foundation for Defense of Democracies. Helsinki, 2018. URL: <https://view.24mags.com/mobilev/bbc43250c51aa3c0b599cb18066f3c#/page=1>
8. Harjanne A., Muilu E., Pääkkönen J., Smith H. (2018) Helsinki in the era of hybrid threats

– Hybrid influencing and the city. – Helsinki, Finland: Hybrid CoE.  
URL:[https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti\\_eng\\_020818\\_netti.pdf](https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_eng_020818_netti.pdf)

### **Додаткова інформація**

Детальнішу інформацію щодо методів навчання, форм оцінювання, самостійної роботи та повного списку літератури наведено у Робочій програмі навчальної дисципліни.

### **ПОЛІТИКА ДИСЦИПЛІНИ**

#### **Щодо академічної доброчесності**

Дотримання академічної доброчесності засновується на ряді положень та принципів академічної доброчесності, що регламентують діяльність здобувачів вищої освіти та викладачів ДУІТ:

[Кодекс академічної доброчесності Державного університету інфраструктури та технологій](#)

[Положення про систему забезпечення академічної доброчесності у Державному університеті та технологій](#)

[Положення про Комісію з академічної доброчесності у ДУІТ та Комісію з етики та управління конфліктами у сфері академічної доброчесності у ДУІТ](#)

Порушення [Кодексу академічної доброчесності ДУІТ](#) є серйозним порушенням, навіть якщо воно є ненавмисним.

Списування під час контрольних заходів заборонені.

Усі письмові роботи, виконані в електронному вигляді (реферати), перевіряються на наявність плагіату згідно з [Положенням про порядок перевірки навчальних, кваліфікаційних, науково-методичних наукових та інших робіт на наявність ознак академічного плагіату у ДУІТ](#). У випадках виявлення порушення – реагування відповідно до [Кодексу академічної доброчесності ДУІТ](#).

#### **Щодо відвідування**

Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (хвороба, міжнародне стажування, індивідуальний графік тощо) навчання може відбуватися в онлайн (або змішаній) формі за погодженням із деканом факультету.

#### **Неформальна освіта**

Можливість зарахування результатів неформальної освіти регламентується «[Положенням про визнання результатів навчання, отриманих у неформальній освіті здобувачами вищої освіти ДУІТ](#)».