Силабус освітнього компонента
Програма навчальної дисципліни

Гібридні війни та національна безпека

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
8

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Гибридні війни та національна безпека" є нормативною навчальною дисципліною. Гибридні війни та національна безпека є актуальними темами в сучасному світі, і їх розуміння є важливим для аналізу геополітичних конфліктів та захисту національної безпеки. Дисципліна спрямована на формування у фахівців розуміння вивчення теорій інформаційного протиборства під впливом комунікаційних технологій; з'ясування проблем спеціального інформаційного впливу; вивчення стратегій і практики проведення спеціальних інформаційних операцій; дослідження комунікативного виміру методології, планування, здійснення інформаційних операцій; формування навичок використання методики та методології протидії інформаційним операціям.

Мета та цілі дисципліни

Ознайомити студентів з історією виникнення та розвитку методології гибридних війн та національної безпеки, концептуально-теоретичними та практичними основами проведення гибридних та інформаційних війн; дати студентам базові теоретичні знання для розуміння природи інформаційного протистояння й практичні навички для оцінювання властивостей інформаційних потоків.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН4. Вільно спілкуватися державною мовою.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 20 год., лабораторні роботи – 20 год., самостійна робота – 80 год.

Передумови вивчення дисципліни (пререквізити)

Національна безпека держави, Менеджмент інформаційної безпеки, Комп'ютерні мережі.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до гібридних воєн. Ознайомлення з поняттям гібридної війни, її історичними витоками, особливостями та сучасними формами прояву.	2
Тема 2. Типи та інструменти гібридних загроз. Класифікація гібридних загроз — кібератаки, дезінформація, економічний тиск, підривні операції; огляд інструментів, що використовуються у таких війнах.	2
Тема 3. Гібридні війни у сучасному світі. Розгляд конкретних кейсів застосування гібридних стратегій у міжнародній політиці та їх впливу на безпеку держав.	2
Тема 4. Гібридні загрози та кібербезпека. Визначення ролі кіберпростору у гібридних конфліктах, аналіз прикладів кібератак та кібероперацій у глобальному контексті.	2
Тема 5. Дезінформація, пропаганда і соціальні медіа. Дослідження інформаційного впливу, методів створення та поширення фейкових новин, використання соцмереж для маніпуляції суспільною думкою.	2
Тема 6. Економічні інструменти гібридної війни. Вивчення фінансових методів впливу — санкцій, валютного тиску, блокування ресурсів та енергетичної залежності.	2
Тема 7. Інформаційна війна та кібератаки. Аналіз сучасних інформаційних кампаній, хактивізму, методів впливу через цифрові технології та ЗМІ.	2
Тема 8. Енергетична безпека як ціль гібридних операцій. Дослідження атак на енергетичну інфраструктуру, кіберзагроз у сфері енергетики та їх наслідків для національної безпеки.	2
Тема 9. Міжнародне співробітництво у протидії гібридним загрозам. Огляд діяльності НАТО, ЄС, ООН та інших структур у сфері виявлення, реагування та запобігання гібридним війнам.	2
Тема 10. Захист і стратегії протидії гібридним загрозам. Вивчення державних і корпоративних стратегій безпеки, методів побудови стійкості до гібридних атак та прогнозів майбутніх викликів.	2
Загальна кількість годин	**20**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Вивчення та аналіз основних видів гібридних війн. Ознайомлення з класифікацією гібридних воєн, їхніми характеристиками та історичними прикладами.	2	0,1
Тема 2. Підходи, сутність та особливості гібридної війни. Аналіз основних підходів до вивчення гібридних конфліктів та особливостей їхньої реалізації.	2	0,1
Тема 3. Аналіз кіберзагроз. Призначення, наслідки, протидія. Вивчення основних видів кіберзагроз, їхнього впливу на безпеку держави та методів протидії.	2	0,1
Тема 4. Міжнародний досвід протидії гібридним загрозам. Дослідження практик інших країн у сфері виявлення, оцінки та нейтралізації гібридних загроз.	2	0,1
Тема 5. Гібридні загрози та національна стратегія. Аналіз взаємозв'язку між гібридними загрозами та формуванням національних стратегій безпеки.	2	0,1
Тема 6. Національна стійкість до гібридних загроз. Вивчення факторів і механізмів підвищення стійкості держави до комплексних загроз.	2	0,1
Тема 7. Розгляд заходів та стратегій для захисту від гібридних загроз національної безпеки. Практичний аналіз заходів і стратегій протидії, спрямованих на збереження національної безпеки.	4	0,1
Тема 8. Розгляд регіональних тенденцій розвитку гібридних війн. Дослідження регіональних особливостей та тенденцій розвитку гібридних конфліктів у світі.	4	0,1
Загальна кількість годин	**20**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Природа, структура та інструменти гібридних загроз. Аналіз сутності гібридних загроз, їх видів та методів реалізації; огляд основних інструментів гібридних операцій і прикладів сучасних гібридних дій.	0,1
Тема 2. Протидія гібридним загрозам та роль інформаційної безпеки. Вивчення методів протидії гібридним загрозам, впливу дезінформації та соціальних медіа; роль кібербезпеки та міжнародного співробітництва у забезпеченні національної безпеки.	0,1

Загалом	$\sum_{i=1}^{m} b_i=0,2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Психологічні операції у гібридних війнах. Вивчення методів психологічного впливу на населення та військові колективи, маніпуляцій суспільною свідомістю.	8
Тема 2. Використання соціальних мереж у гібридних конфліктах. Аналіз способів поширення дезінформації та пропаганди через цифрові платформи.	8
Тема 3. Енергетична безпека та гібридні загрози. Дослідження загроз для критичної енергетичної інфраструктури під час гібридних атак.	8
Тема 4. Фінансові інструменти у гібридній війні. Розгляд економічного тиску та санкцій як складової гібридного впливу.	8
Тема 5. Кібер-розвідка та контррозвідка. Ознайомлення з методами збору та захисту інформації у кіберпросторі.	8
Тема 6. Дезінформація та фейкові новини. Вивчення технологій створення та поширення неправдивої інформації, її вплив на національну безпеку.	8
Тема 7. Інформаційна гібридна безпека держави. Аналіз засобів захисту від інформаційних атак та забезпечення достовірності даних.	8
Тема 8. Військові аспекти гібридних воєн. Дослідження тактики та стратегії використання військових ресурсів у гібридних конфліктах.	8
Тема 9. Правові аспекти протидії гібридним загрозам. Вивчення законодавчого регулювання та міжнародного права у сфері захисту від гібридних атак.	8
Тема 10. Роль міжнародних організацій у протидії гібридним загрозам. Аналіз діяльності НАТО, ООН та інших організацій щодо запобігання та нейтралізації гібридних загроз.	8
Загальна кількість годин	**80**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Парахонський Б. О., Яворська Г. М. Онтологія війни і миру: безпека, стратегія, смисл. – Київ : НІСД, 2019. – 560 с.
https://chtyvo.org.ua/authors/Parakhonskyi_Borys/Ontolohiia_viiny_i_myru_bezpeka_stratehiia_smysl/
3. Магда Є.В. Гібридна війна – вижити і перемогти. Харків : Віват, 2015. 604 с.
https://balka-book.com/files/2017/06_10/12_24/u_files_store_6_68818.pdf?srsltid=AfmBOooBf2b0UpUhaqthMVBc9ycOTQSnnFXBKvA4kcPcGtWmGOdcCHPF
4. Гібридна війна: сутність, виклики та загрози: зб. матер. круглого столу (Київ, 8 липня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 189 с.
https://nasbu.edu.ua/uploads/p_57_28744724.pdf
5. Курбан О.В. Сучасні інформаційні війни в мережевому онлайн просторі. – Київ: ВІКНУ, 2016. - 286 с.
http://www.interinf.chnu.edu.ua/res//interinf/Inf%20vijny.pdf
6. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ: Книголов, 2019. 384 с.
7. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. Київ: НІСД, 2016. 109 с.
https://niss.gov.ua/publikacii/analitichni-dopovidi/informaciyni-vikliki-gibridnoi-viyni-kontent-kanali-mekhanizmi

Додаткова література

8. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Роман КОРОЛЬОВ