Силабус освітнього компонента
Програма навчальної дисципліни

Гибридні війни та національна безпека

Шифр та назва спеціальності
257 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Управління інформаційною безпекою

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), Обов'язкова

Семестр
8

Мова викладання
Українська

Викладачі, розробники

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

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» 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 роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

37137 11
КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

Результати навчання

ПРН–3. 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.
ПРН-4. Вільно спілкуватися державною мовою.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. 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 – 24 год., лабораторні роботи – 36 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

Інформаційна безпека держави, Національні інформаційні ресурси, Менеджмент інформаційної безпеки, Введення в 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

Теми лекційних занять

Тема 1. Вступ до гібридних воєн.
Огляд поняття гібридних війн, їхній визначення та історичний контекст.
Тема 2. Типи гібридних загроз.
Аналіз різних типів гібридних загроз, таких як кібератаки, дезінформація, фінансовий тиск і субверсія.
Тема 3. Гібридні загрози в сучасному світі.
Дослідження конкретних прикладів гібридних загроз, які вплинули на національну безпеку різних країн.
Тема 4. Інструменти гібридної війни.
Розгляд різних інструментів і методів, які використовуються для проведення гібридних операцій.
Тема 5. Гібридні війни і кібербезпека.
Аналіз взаємозв'язку між гібридними загрозами і кібербезпекою.
Тема 6. Дезінформація та пропаганда.
Розгляд впливу дезінформації і пропаганди на національну безпеку.
Тема 7. Фінансовий тиск і санкції.
Вивчення використання фінансового тиску та санкцій у гібридних операціях.
Тема 8. Роль соціальних медіа в гібридних війнах.
Дослідження впливу соціальних медіа на поширення дезінформації та маніпуляцію громадською думкою.
Тема 9. Інформаційна війна та кібератаки.
Огляд сучасних прикладів інформаційної війни та кібератак.
Тема 10. Гібридні загрози та енергетична безпека.
Вивчення можливого впливу гібридних загроз на енергетичну інфраструктуру.
Тема 11. Гібридні загрози у кіберпросторі.
Аналіз кіберзагроз, їхні призначення і наслідки.
Тема 12. Захист від гібридних загроз.
Розгляд заходів та стратегій для захисту від гібридних загроз національної безпеки.
Тема 13. Міжнародне співробітництво в боротьбі з гібридними загрозами.
Дослідження ролі міжнародних організацій і співробітництва між країнами у боротьбі з гібридними війнами.
Тема 14. Юридичні та етичні аспекти гібридних війн.
Розгляд правових та етичних питань, пов'язаних з гібридними загрозами.
Тема 15. Роль інформаційної безпеки в захисті від гібридних загроз.
Вивчення ролі інформаційної безпеки у забезпеченні національної безпеки в умовах гібридних загроз.
Тема 16. Стратегії та прогнози для майбутнього.
Обговорення можливих майбутніх розвитків у гібридних війнах та національній безпеці.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Вивчення та аналіз основних видів гібридних війн.
Тема 2. Підходи, сутність та особливості гибридної війни.
Тема 3. Аналіз кіберзагроз. Призначення, наслідки, протидія.
Тема 4. Міжнародний досвід протидії гібридним загрозам.
Тема 5. Гібридні загрози та національна стратегія.
Тема 6. Національна стійкість до гібридних загроз.
Тема 7. Розгляд заходів та стратегій для захисту від гібридних загроз національної безпеки.
Тема 8. Розгляд регіональних тенденцій розвитку гібридних війн.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

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 віна – 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

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•залік: 40% семестрової оцінки.

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

Студент 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 28.08.2024 Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 Гарант ОП
Роман КОРОЛЬОВ