Силабус освітнього компонента
Програма навчальної дисципліни

Державне управління національним інформаційним простором

Шифр та назва спеціальності
281 – Публічне управління та адміністрування

Інститут
Навчально - науковий інститут соціально - гуманітарних технологій

Освітня програма
Цифрове врядування

Кафедра
Соціології і публічного управління (305)

Рівень освіти
Бакалавр

Тип дисципліни
Спеціальна (фахова), вибіркова ,

Семестр
5

Мова викладання
Українська

Викладачі, розробники

МОРОЗ Володимир Михайлович

volodymyr.moroz @khpi.edu.ua
Мороз Володимир Михайлович
Доктор наук з державного управління, професор, завідувач кафедри соціології і публічного управління НТУ «ХПІ».
Автор понад 300 наукових та навчально-методичних праць. Провідний лектор з дисциплін: «Ризик-менеджмент в системі прийняття управлінських рішень», «Методологія організації наукових досліджень та методика написання наукових текстів», «Глобалізація і політика національної безпеки». Член спеціалізованої вченої ради Д64.707.03.
Детальніше про викладача на сайті кафедри
http://web.kpi.kharkov.ua/sp/profesors-ko-vikladats-kij-sklad

ТЕРЕЩЕНКО Діна Акрамівна

dina.tereshchenko@khpi.edu.ua
Докторка наук з державного управління, професорка, професорка кафедри соціології і публічного управління НТУ «ХПІ».
Науково-педагогічний стаж - понад 20 років. Досвід роботи в органах публічної влади - понад 12 років. Авторка понад 200 наукових і навчально-методичних публікацій.
Детальніше про викладача на сайті кафедри
http://web.kpi.kharkov.ua/sp/profesors-ko-vikladats-kij-sklad

Загальна інформація

Анотація

Навчальна дисципліна «Державне управління національним інформаційним простором» присвячена вивченню теоретичних засад, стратегічних пріоритетів та практичних механізмів регулювання вітчизняного інформаційного середовища. Курс охоплює такі ключові аспекти: формування та трансформація національного інформаційного простору в умовах глобалізації; стратегії розвитку інформаційного суспільства та механізми реалізації державної інфополітики на національному та регіональному рівнях; повноваження та функції органів державної влади, що здійснюють управління та нагляд в інформаційній галузі; аналіз нормативно-правової бази, що визначає правила гри для медіа, телекомунікацій та цифрових платформ; захист національного суверенітету в цифровому вимірі, протидія дезінформації, пропаганді та кіберзагрозам; розвиток електронного урядування та інструментів прямої комунікації між державою і громадянським суспільством.

Мета та цілі дисципліни

формування у здобувачів вищої освіти комплексного розуміння ролі держави в регулюванні інформаційної сфери, в управлінні національними інформаційними ресурсами та інформаційними процесами, у забезпеченні доступу до публічної інформації та захисту інформації з обмеженим доступом, а також особливостей розвитку інформаційного суспільства в Україні та світі..

Формат занять

Лекції, практичні заняття, консультації. Підсумковий контроль – екзамен.

Компетентності

ЗК1. Здатність вчитися та оволодівати сучасними знаннями.
ЗК8. Вміння виявляти, ставити та вирішувати проблеми.
ЗК9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел..
ЗК11. Здатність спілкуватися іноземною мовою.
СК4. Здатність використовувати в процесі підготовки і впровадження управлінських рішень сучасні ІКТ.
СК5. Здатність використовувати систему електронного документообігу.
СК6. Здатність здійснювати інформаційно-аналітичне забезпечення управлінських процесів із використанням сучасних інформаційних ресурсів та технологій.
СК14. Здатність визначати стан електронної готовності щодо впровадження електронного урядування на місцевому, регіональному та загальнодержавному рівнях.

Результати навчання

РН5. Знати стандарти, принципи та норми діяльності у сфері публічного управління та адміністрування.
РН9. Знати основи електронного урядування.
РН10. Уміти користуватися системою електронного документообігу.
РН11. Уміти здійснювати пошук та узагальнення інформації, робити висновки і формулювати рекомендації в межах своєї компетенції.
РН20. Уміти використовувати технології та інструменти електронного урядування і електронної демократії.
РН21. Використовувати інформаційні й комунікаційні технології для вирішення складних спеціалізованих задач і проблем професійної діяльності; знати принципи, технології і прийоми створення усних і письмових текстів різних стилів державною та іноземною мовами..

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): денна форма: лекції – 32 год., практичні заняття – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Дисципліни, вивчення яких спирається на дану дисципліну: «Вища математика», «Теорія організації», «Вступ до спеціальності. Ознайомча практика», «Соціально-демографічна статистика», «Організаційно-правові засади публічного управління», «Основи публічного управління та адміністрування», «Державне та регіональне управління».

Особливості дисципліни, методи та технології навчання

Лекції проводяться інтерактивно з використанням мультимедійних технологій. На практичних заняттях використовується проєктний підхід до навчання, ігрові методи, акцентується увага на застосуванні інформаційних технологій. На практичних заняттях використовуються: ігрове проєктування; робота із законодавчими актами та іншими нормативно-правовими документами; виступи-презентації; опрацювання лекційного матеріалу та фахової літератури.
Навчання передбачає використання словесних (лекція, розповідь, пояснення, інтерактивна бесіда), наочних (ілюстрація, демонстрація, спостереження) та практичних (практична робота, розв'язання задач, тренувальні і творчі вправи) методи навчання. Під час лекційних занять використовуються презентації, які поєднують словесні та наочні методи навчання, що дає можливість здобувачам вищої освіти акумулювати знання. Під час практичних занять застосовуються словесні та практичні методи навчання, які спрямовані на формування у здобувачів вищої освіти здібностей пізнання, а саме: інтерактивне обговорення тем, розв'язання практичних задач та розбір теоретичних вправ, дискусії, індивідуальна та командна форми роботи, вивчення готових кейсів.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Основи інформаційної безпеки.
Основні положення інформаційної безпеки. Законодавчий та адміністративний рівні інформаційної безпеки. Організаційний та технічний рівні інформаційної безпеки. Програмно-технічний рівень інформаційної безпеки. Інформаційна безпека держави. Основи державної політики у сфері інформаційної безпеки України. Досвід забезпечення інформаційної безпеки в державах ЄС, США.
Тема 2. Сутність кібербезпеки держави та основні проблеми її забезпечення.
Сутність кібербезпеки держави та основні проблеми її забезпечення. Загрози в сфері кібербезпеки за стандартами країн-членів НАТО. Кібернетичні дії та їх особливості. Основні принципи дій в кіберпросторі та в електронних війнах за стандартами. Операції в кіберпросторі та електронній війні. Досвід провідних країн світу щодо забезпечення кібербезпеки держави.
Тема 3. Суспільні трансформації в умовах інформаційного суспільства.
Інформація та інформаційні ресурси як об'єкт державної політики та управління. Державна інформаційна політика щодо розвитку інформаційного суспільства та інформаційної сфери. Державне управління в умовах розвитку інформаційного суспільства. Органи управління в інформаційній сфері. Забезпечення доступу громадян до інформації як напрям державної інформаційної політики. Інформаційна безпека держави.
Тема 4. Основні загрози національній безпеці держави в інформаційній сфері.
Класифікація загроз: внутрішні та зовнішні чинники дестабілізації національного інфопростору. Спеціальні інформаційні операції та ПсО (психологічні операції): сутність, етапи, об'єкти впливу. Канали реалізації загроз: від класичних медіа до месенджерів та deep-web. Феномен «постправди» та деструктивний вплив пропаганди на державні інститути. Методика моніторингу та раннього виявлення загроз в інформаційному середовищі.
Тема 5. Стратегічні цілі та завдання інформаційної боротьби.
Ієрархічні рівні інформаційної боротьби: стратегічний, оперативний та тактичний. Об'єкти інформаційного протиборства: свідомість населення, система прийняття рішень, технічна інфраструктура. Стратегічні комунікації (StratCom) як інструмент державної протидії агресії. Наративне домінування: формування та просування національного порядку денного. Етика та міжнародне право в контексті інформаційної боротьби.
Тема 6. Державне управління інформаційною безпекою.

Державний контроль та аудит стану захищеності інформаційних систем. Інформаційно-аналітичне забезпечення прийняття управлінських рішень в умовах кризи. Механізми державно-приватного партнерства у сфері інформаційної безпеки. Кризовий менеджмент при виникненні масштабних інформаційних та кіберінцидентів. Підготовка кадрів та формування культури інформаційної гігієни серед державних службовців.

Тема 7. Національний інформаційний простір.

Структура та межі національного інформаційного простору в епоху транскордонних цифрових потоків. Особливості розвитку українського інфопростору в умовах воєнного стану.Регулювання діяльності соціальних мереж та OTT-платформ на державному рівні. Інструменти захисту мовно-культурного простору та підтримки національного інформаційного продукту. Суверенітет у цифровому світі: виклики великих технологічних корпорацій (Big Tech).

Тема 8. Штучний інтелект як інструмент інформаційної війни.

Робота штучного інтелекту з інформацією: створення та опрацювання контенту, виявлення інформаційних трендів, аналіз зображень тощо. Потенціал штучного інтелекту для створення і поширення дезінформації. Штучний інтелект для відстеження та аналізу поведінки користувачів у соціальних мережах для визначення ключових тем та формування впливових стратегій. Створення захищеного національного інформаційного простору за допомогою технологій штучного інтелекту. Алгоритмічні системи штучного інтелекту у виявленні та аналізі фейкових новин та пропагандистської інформації. Штучний інтелект для захисту від кібератак і кіберзагроз..

Теми практичних занять

Тема 1. Основи інформаційної безпеки.

Аналіз Стратегії інформаційної безпеки України: цілі та індикатори виконання. Розробка проекту адміністративного регламенту щодо захисту персональних даних в умовній державній установі. Порівняльний кейс-стаді: зіставлення стандартів ISO/IEC 27001 та нормативів ДСЗЗІ України. Моделювання системи технічного захисту: розробка переліку організаційних заходів для забезпечення програмно-технічного рівня безпеки об'єкта критичної інфраструктури. Адаптація досвіду ЄС/США: підготовка пропозицій щодо імплементації директив NIS 2 в українське законодавство.

Тема 2. Сутність кібербезпеки держави та основні проблеми її забезпечення.

Класифікація кіберінцидентів: робота з таксономією загроза за стандартами НАТО (аналіз реальних звітів CERT-UA). Симуляція реагування на кібератаку: алгоритм дій органу державної влади при виявленні втручання в ІТС. Розробка карти кіберзагроз: ідентифікація вразливостей в електронних реєстрах та системах документообігу. Кібергігієна в публічному управлінні.

Тема 3. Суспільні трансформації в умовах інформаційного суспільства.

Аудит надання публічної інформації: перевірка офіційних веб-порталів органів влади на відповідність вимогам щодо «відкритих даних». Проектування моделі електронного урядування: розробка структури нової електронної послуги з урахуванням захисту прав громадян. Аналіз діяльності регуляторних органів: оцінка ефективності Нацради з питань телебачення і радіомовлення в сучасних умовах. Механізми залучення громадян: практичне використання інструментів е-петицій та громадського бюджету.

Тема 4. Основні загрози національній безпеці держави в інформаційній сфері.

Аналіз ІПСО (інформаційно-психологічних операцій): деконструкція конкретного кейсу (мета, канали, наративи, об’єкти). Робота з OSINT-інструментами: базові навички перевірки джерел інформації та верифікації контенту. Побудова системи моніторингу: вибір критеріїв для раннього виявлення дестабілізуючого контенту в соцмережах. Розробка контрнаративів: створення комунікаційної стратегії для спростування масштабного фейку.

Тема 5. Стратегічні цілі та завдання інформаційної боротьби.

Формування StratCom-пакету: розробка ключових повідомлень (key messages) для підтримки державної реформи. Моделювання «наративного домінування»: рольова гра з просування національного порядку денного в міжнародному медіапросторі. Етичний аудит інформаційної боротьби: аналіз межі між контрпропагандою та обмеженням свободи слова. Планування операцій StratCom: координація дій різних державних інституцій для досягнення єдиної мети.

Тема 6. Державне управління інформаційною безпекою.

Розробка плану безперервності діяльності (BCP): забезпечення функціонування органу влади під час блекауту або масованої атаки. Аудит інформаційної захищеності: проведення (умовного) самообстеження системи безпеки державної установи. Кейс «Державно-приватне партнерство»: розробка меморандуму про співпрацю між держструктурою та IT-компанією. Комунікативний менеджмент у кризі: підготовка брифінгу для ЗМІ після масштабного витоку даних.

Тема 7. Національний інформаційний простір.

Механізми взаємодії з Big Tech: розробка офіційного запиту до Meta/Google щодо видалення шкідливого контенту. Захист мовно-культурного простору: моніторинг дотримання квот та аналіз інструментів підтримки україномовного продукту. Регулювання Telegram та TikTok: дискусія-аналіз щодо балансу між безпекою та правами людини.Цифровий суверенітет: оцінка ризиків використання іноземного ПЗ у критичній інфраструктурі.

Тема 8. Штучний інтелект як інструмент інформаційної війни.

Детекція фейків за допомогою ШІ: тестування інструментів (Deepware чи аналогів) для виявлення дипфейків. Генерація контенту для держкомунікацій: практичне використання ШІ для підготовки роз'яснювальних матеріалів та аналітики. Моделювання ШІ-загроз: розробка сценарію захисту від автоматизованої ферми ботів, керованої штучним інтелектом. ШІ-аналітика трендів: використання алгоритмів для прогнозування соціальної реакції на управлінські рішення.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

Самостійна робота

Програма самостійної роботи передбачає систематичне опрацювання лекційного матеріалу та ретельну підготовку до семінарських занять разом із поглибленим вивченням окремих тем і питань, які не виносяться на лекційне обговорення задля стимулювання дослідницької активності студентів. Важливою складовою позааудиторної діяльності є самостійний аналіз додаткових джерел, серед яких ключове місце посідають офіційні вебпортали органів державної влади та судових інституцій, що дозволяє здобувачам відстежувати реальні кейси інформаційно-аналітичного супроводу публічного управління.

Окремим обов'язковим видом самостійної навчальної діяльності є підготовка наукового реферату за обраною тематикою. У процесі написання реферату студенти повинні продемонструвати вміння логічно викладати результати теоретичного пошуку, дотримуватися вимог до академічної доброчесності та формулювати власні висновки щодо вдосконалення аналітичних процесів у сучасній державній політиці.

Література та навчальні матеріали

Основна література:

1. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: Підручник. К.: ДУТ, 2015. 288 с.
2. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем: підручник. К.: Видавнича група BHV, 2009. 608 с.
3. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.
4. Гур'єв В. І., Мехед Д. Б., Ткач Ю. М., Фірсова І. В. Інформаційна безпека держави : навч. посіб. Ніжин, 2018. 166 с. URL: https://ir.stu.cn.ua/handle/123456789/19246.
5. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони. Підручник. Одеса.: ОНАЗ, 2018. 228 с.
6. Семенченко А. І., Серенок А. О. Публічна політика та управління розвитком інформаційного суспільства та електронного урядування : навч. посіб. К.: ФОП Москаленко О. М., 2017. 80 с. URL: https://library.pdpu.edu.ua/images/2018/NN/demokrat/04.pdf.
7. Чукут С. А., Джига Т. В. Інформаційна політика в Україні : опорний конспект лекцій. К., 2007. 94 с.
8. Digital Transformations in Public International Law / ed. by A. Golia, M. C. Kettemann, R. Kunz. London : Routledge, 2022. 322 p. URL: https://pure.mpg.de/rest/items/item_3560540_1/component/file_3560541/content.

9. Singer P. W., Brooking E. T. LikeWar: The Weaponization of Social Media. New York : Eamon Dolan/Houghton Mifflin Harcourt, 2018. 416 p.
Допоміжна література:
1. Електронне урядування. Інформатизація державного управління : навч. посіб. для студ. вищ. навч. закл. / Ю. Г. Машкаров та ін. ; Нац. акад. держ. упр. при Президентові України. Х. : Вид-во ХарРІДУ НАДУ «Магістр», 2017. 262 с.
2. Костенко О.М. Інформаційно-аналітичний процес: праксеологічний підхід :монографія. Київ, 2013. 204 с.
3. Політична аналітика в державному управлінні: навч. посіб. / С. О. Телешун, Ю. Г. Кальниш, І. В. Рейтерович, О. Р. Титаренко. К.: НАДУ, 2012. 228 с.
5. Цифрове врядування : монографія / О. В. Карпенко, Ж. З. Денисюк, В. В. Наместнік [та ін.] ; за. ред. О. В. Карпенка. Київ : ІДЕЯ ПРИНТ, 2020. 336 с.
6. Янг Е., Куінн Л. Як написати дієвий аналітичний документ у галузі державної політики: практичний посібник / Пер. з англ. С. Соколик. К.: К.І.С., 2003. 130 с.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Критерії оцінювання успішності студента та розподіл балів
100% підсумкової оцінки складаються з результатів оцінювання у вигляді екзамену (40%) та поточного оцінювання (60%).
Екзамен: усне завдання (2 запитання з теорії) та усна доповідь.
Поточне оцінювання: 2 онлайн тести та вирішення практичних завдань (по 30%) та індивідуальне завдання (30%).

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

Дата погодження, підпис
28.06.2024

Завідувач кафедри
Володимир МОРОЗ

Дата погодження, підпис
28.06.2024

Гарант ОП
Діна ТЕРЕЩЕНКО