НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

ННІ Менеджменту, харчових технологій та торгівлі
Кафедра публічного управління та менеджменту організацій

Назва курсу	**Інформаційна гігієна та медіаграмотність у сфері публічного управління**
Мова викладання	*Українська*
Курс та семестр вивчення	для здобувачів третього рівня вищої освіти (доктор філософії) галузі знань 28 – Публічне управління та адміністрування, спеціальність: 281 – Публічне управління та адміністрування 2 курс, 4 семестр
Викладачі	д.держ.упр., професор Ольга Мстиславівна Руденко
Профайли викладачів	https://pumo.stu.cn.ua/kafedra/vikladachi-kafedri/ https://pumo.stu.cn.ua/wp-content/uploads/2023/01/profil-vykladacha_rudenko.pdf
Контакти викладачів	Чернігів, вул. Шевченка, 95, корп.1, каб. 402. Телефон: (046) 665-261; E-mail: kaf_men1@ukr.net

1. **Анотація курсу.** Цифрова держава має свої недоліки, незважаючи на значні переваги, і одне з цих слабких місць – це неналежна, неефективна або в деяких випадках і відсутня кібербезпека. Взагалі, якщо дуже стисло, то кібербезпека є однією з видів інформаційної безпеки, основна мета якої – здійснення захисту державних, персональних, корпоративних даних. Приватна інформація, в тому числі різноманітні бази даних, давно вже стала новою валютою, електронним знаряддям на віртуальному тіньовому ринку попиту і пропозиції. Адже при хакерській атаці несанкціонований витік інформації може завдати значних фінансових збитків компанії, державі або нашкодити особистій репутації окремої приватної особи. Тому особливої актуальності набувають вивчення, у межах дисципліни «Інформаційна гігієна та медіаграмотність у сфері публічного управління», теоретичні, методологічні та практичні основи управління публічною сферою та її складовими для досягнення цілей розвитку суспільства, держави, громади, людського колективу, суб'єктів публічної сфери. Така зацікавленість, а точніше, нагальна необхідність зумовлена діджиталізацією суспільства, розвитком і впровадженням урядом цифрової політики у сфері надання державних послуг, а також, на жаль, одним із головних чинників актуальності цієї теми — збільшенням хакерських атак, особливо підривом електронних державних програм, сервісів і баз даних.

Дисципліна має міждисциплінарний характер.

Змістовний модуль 1. Інформація та масмедіа в системі публічного управління

Тема 1.1 Основні поняття. Типи контенту для публічного управління. Змістовне наповнення понять: медіакомпетентність, медіапростір, медіа, медіакультура, інформація, пропаганда, медіаграмотність. основні теорії медіаосвіти, її зв'язок із іншими навчальними

дисциплінами в системі публічного управління. Класифікація та характеристики контенту в системі публічного управління. Функції і принципи впливу соціальних мереж. Розвиток медіаграмотності в публічному управлінні.

Тема 1.2 Дезінформації та маніпуляції в публічному управлінні. Спотворення в соціальних мережах заголовків та фотофейків. Диференціація методів і способів маніпулятивного впливу різних типів медів на свідомість публічного управлінця. Особливості критичного сприймання й аналізу інформації в публічному управлінні, що подається для широкого загалу. Діяльність професійних комунікантів, їх типи у масовокомунікаційній індустрії. Види ресурси офіційних служб та організацій для перевірки достовірності інформації поданої у медіа просторі. Поняття «фішинг», «смішинг» і «вішинг» для публічного управління.

Тема 1.3. Актуальні проблеми інформаційної гігієни в публічному управлінні. Принципи інформаційної гігієни та безпеки споживача інформації в сучасних реаліях публічного управління. Прийоми створення та розвінчування фальшивої інформації. Алгоритм дій для покращення власної гігієни в соціальних мережах та зменшення ризику потрапляння особистої Інтернет-інформації в чужі руки. Стратегія протидії маніпуляціям та іншим негативним масовим впливам на систему публічного управління.

Змістовний модуль 2. Інформаційна безпека України у сфері публічного управління

Тема 2.1. Теоретико-методологічні аспекти забезпечення інформаційної безпеки у сфері публічного управління. Концептуалізація системи забезпечення інформаційної безпеки у сфері публічного управління. Особливості розвитку інформаційної сфери в розрізі формування конкурентних переваг та безпеки держави. Принципи стратегічного управління інформаційною безпекою. Стратегія забезпечення інформаційної безпеки у сфері публічного управління. Рівень розвитку інформаційної безпеки держави.

Тема 2.2. Тенденції управління інформаційною безпекою в Україні. Фактори забезпечення розвитку інформаційної безпеки у сфері публічного управління. Домінанти державної політики інформаційної безпеки. Сучасні моделі та світовий досвід регулювання розвитку інформаційної сфери публічного управління та перспективи його адаптації в Україні. Нормативно-правовий механізм забезпечення інформаційної безпеки у сфері публічного управління. Методи та важелі державного впливу на інформаційну безпеку держави.

Тема 2.3. Стратегія забезпечення інформаційної безпеки у сфері публічного управління. Алгоритм формування стратегії забезпечення інформаційної безпеки у сфері публічного управління. Модель реалізації забезпечення інформаційної безпеки у сфері публічного управління. Методичний інструментарій виявлення загроз інформаційній безпеці у сфері публічного управління.

Змістовний модуль 3. Інформаційно-комунікаційні технології як основа інформаційного суспільства та ефективного публічного управління

Тема 3.1. Особливості функціонування публічного управління в сучасному інформаційному просторі. Поняття інформаційно-комунікаційних технологій. Формування інформаційного суспільства в Україні. Сучасний стан публічного управління в умовах інформаційного суспільства. Основні стратегічні цілі розвитку інформаційного суспільства в Україні. Національна політика розвитку інформаційного суспільства в Україні.

Тема 3.2. Цифрові технології у сфері публічного управління. Цифрова трансформація управлінської діяльності. Впровадження цифрових технологій в організаціях та установах публічного управління. Стратегія цифрових технологій у діяльності органів публічного управління.

Тема 3.3. Інструменти цифрового маркетингу в умовах трансформації комунікацій суб'єктів публічного управління. Розвиток інформаційно-комунікаційних технологій та діджиталізація процесів публічного управління. Сучасні інструменти маркетингу, які суб'єкти управління застосовують у цифровому середовищі. Перспективні напрями розвитку інструментів цифрового маркетингу у сфері публічного управління.

Змістовний модуль 4. Медіакультура у сфері публічного управління

Тема 4.1. Медіакультура як особливий тип культури інформаційного суспільства. Особливості змісту поняття «медіакультура». Генеза феномену «медіакультура». Медіаосвіта і медіаграмотність як необхідні компоненти медіакультури.

Тема 4.2. Інформаційний ринок і механізм його функціонування. Поняття та структура інформаційного ринку. Механізм функціонування інформаційного ринку. Суб'єкти інформаційного ринку. Поняття інформаційного виробництва. Особливості кінцевого продукту інформаційного виробництва. Особливості процесу праці в інформаційному виробництві.

Тема 4.3. ФінТех у сфері публічного управління України: огляд та проблемні питання. Проблеми розвитку ФінТех у сфері публічного управління. Напрямки застосування ФінТех у сфері публічного управління. Вимоги щодо безпечності і стабільності роботи цифрового банкінгу. Перспективні напрямки адаптації ФінТех технологій до потреб системи публічного управління.

Змістовний модуль 5. Сутність та тенденції розвитку ринку цифрових технологій в публічному управлінні

Тема 5.1. Цифрові публічні послуги та моделювання процесів їх надання. Електронний документообіг в органах публічного управління: можливості та обмеження дистанційної роботи. Е-урядування базовими галузями. Управління розвитком е-урядування. Дотримання безпеки роботи з інформацією у відділеному доступі. Інструменти для віддаленого управління проєктами та тайм-менеджменту. Організація комунікацій в умовах віддаленого доступу.

Тема 5.2. Організація діяльності державних службовців в умовах цифровізації. Інструменти електронного врядування. Механізми впровадження електронної демократії. Електронні інструменти просторового планування. Електронні звернення.

Тема 5.3. Кібербезпека та управління викликами. Особливості управління викликами кібербезпеки. Основні поняття і визначення. Національна система. кібербезпеки України. Теоретичні основи побудови систем виявлення та реагування на кіберінциденти.

2. Мета та цілі курсу. *Метою навчальної дисципліни* є формування інформаційної та медіакультури у здобувачів, підвищення рівня компетентностей при вирішенні завдань інформаційної комунікації на державній службі, реагування та протидії дезінформації задля прийняття ефективних публічно-управлінських рішень в умовах невизначеності та змін, посилення інформаційної безпеки в сучасних умовах.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (ЗК) та фахові (СК) компетентності, передбачені освітньою програмою:

ЗК 5. Здатність налагоджувати діалогову взаємодію з широкою науковою спільнотою, співробітництво, ефективну комунікацію влади та громадськості, працювати у міжнародному контексті.

ЗК 6. Здатність до науково-педагогічної діяльності, організації і здійснення освітнього процесу.

СК 10. Здатність приймати обґрунтовані управлінські рішення, в тому числі, в конфліктних ситуаціях, умовах невизначеності, криз та загроз, а також з метою їх запобігання, передбачати й прогнозувати імовірні ризики у різних сферах суспільного буття.
СК 11. Здатність до розробки науково обґрунтованих рекомендацій щодо вдосконалення публічного управління та адміністрування з урахуванням сучасних викликів і загроз.
СК 12. Здатність до комунікативного партнерства на наддержавному, національному, регіональному, місцевому рівнях, на рівні організації державною та іноземними мовами, вміння спілкуватися в іншомовному науковому і професійному середовищах.

3.Очікувані результати навчання

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:
ПРН 7. Уміти розробляти нові підходи та адаптувати кращі практики електронної демократії для вирішення сучасних питань публічної комунікації, інформаційної безпеки в системі публічного управління та адміністрування.

4. Обсяг курсу. Загальна кількість кредитів – 5 (загальна кількість годин - 150); кількість годин самостійної робити – 110.

Вид заняття	**Загальна кількість годин**
Лекції	26
Семінарські заняття	24
Самостійна робота	100

Форма проведення занять – лекційні, практичні, самостійна робота – з використанням системи дистанційного навчання Moodle, літератури, відеоматеріалів.

5. Пререквізити. Передумовою вивчення дисципліни є базові знання з дисциплін: «Публічна політика»; «Іноземна мова для наукового спілкування»; «Методологія, організація та технологія наукових досліджень».

6. Система оцінювання та вимоги. Поточний контроль – до 60 балів, в тому числі: практичні заняття – до 50 балів, підсумковий модульний контроль – до 10 балів

Семестровий контроль у вигляді іспиту проводиться під час сесії у вигляді усних відповідей на запитання (максимум 40 балів). Оцінка за результатами вивчення дисципліни формується шляхом додавання підсумкових результатів поточного контролю до оцінки за іспит.

Загальна система оцінювання курсу	*Активна участь в роботі впродовж семестру (виконання тематичних завдань, виконання індивідуальних практичних завдань) /залік - 60/40*
Семінарські заняття	*Підготовка усних відповідей з лекційного матеріалу, відповідь на питання самостійного опрацювання, виконання практичних завдань*
Умови допуску до підсумкового контролю	*Наявність конспекту лекцій, активність протягом навчального семестру, мінімальна кількість балів 21.*

Поточний контроль

Модуль за тематичним планом дисципліни та форма контролю	Кількість балів за видами робіт	
	Усні відповіді, підготовленість до	Повнота та своєчасність

	практичних занять	виконання завдань
Змістовий модуль 1. **Інформація та масмедіа в системі публічного управління**	0…3	0…10
Змістовий модуль 2. **Інформаційна безпека України у сфері публічного управління**	0…3	0…5
Змістовий модуль 3. **Інформаційно-комунікаційні технології як основа інформаційного суспільства та ефективного публічного управління**	0…3	0…10
Змістовий модуль 4. **Медіакультура у сфері публічного управління**	0…3	0…5
Змістовий модуль 5. **Сутність та тенденції розвитку ринку цифрових технологій в публічному управлінні**	0…3	0…5
Підсумкова поточна оцінка за семестр	15	35

Підсумковий модульний контроль

Модуль за тематичним планом дисципліни та форма контролю	**Кількість балів**
Змістовий модуль 1. **Інформація та масмедіа в системі публічного управління** (тестові завдання)	0…2
Змістовий модуль 2. **Інформаційна безпека України у сфері публічного управління** (тестові завдання)	0…2
Змістовий модуль 3. **Інформаційно-комунікаційні технології як основа інформаційного суспільства та ефективного публічного управління** (тестові завдання)	0…2
Змістовий модуль 4. **Медіакультура у сфері публічного управління** (тестові завдання)	0…2
Змістовий модуль 5. **Сутність та тенденції розвитку ринку цифрових технологій в публічному управлінні** (тестові завдання)	0…2

Підсумкова семестрова оцінка

Види робіт	Кількість балів
Поточний контроль	0…50
Підсумковий модульний контроль	0…10
Залік	0…40
Разом	0…100

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		екзамен/диференційований залік	залік
90 – 100	**A**	Відмінно	зараховано
82-89	**B**	Добре	
75-81	**C**		
66-74	**D**	задовільно	
60-65	**E**		
0-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

7. Політики курсу. Обов'язкова активна участь в обговоренні проблемних питань, участь у всіх видах контролю.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі передбачених робочою програмою всіх видів навчальної роботи, має невідпрацьовані практичні роботи або не набрав мінімально необхідну кількість балів, він не допускається до складання заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому Положенням про поточне та підсумкове оцінювання знань здобувачів НУ "Чернігівська політехніка". Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний залік складається з двома теоретичними та одним практичним питаннями.

До загальної політики курсу відноситься дотримання принципів відвідування занять очно у відповідності до затвердженого розкладу, крім випадків карантину (коли заняття проводяться дистанційно через Інтернет), а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл. Запорукою успішного вивчення дисципліни є активність та залучення під час проведення практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу (принципи описані у Кодексі академічної доброчесності Національного університету «Чернігівська політехніка» за посиланням: https://www.stu.cn.ua/staticpages/akadem-dobrochesnist/). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Політика дедлайнів

Своєчасність здачі завдань оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачам вищої освіти курсу можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, статті на науково-практичних конференціях тощо.

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час проведення підсумкового контролю.

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти за даною спеціальністю з освітніх компонент, спрямованих на отримання компетентносте з курсу, можуть бути перезараховані викладачем у відповідності до положення Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка» шляхом співставлення отриманих програмних результатів навчань та компетентносте. У випадку проходження подібного курсу з інших спеціальностей перезараховані можуть бути лише теми, зазначені в курсі відповідно до змістових модулів.

8. Рекомендована література

Базова

1. Інформаційна безпека. Підручник В.В.Остроухов, М.М.Присяжнюк, О.І.Фармагей, М.М.Чеховська та ін.; під ред. В.В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.
2. Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця: монографія / [В. Азарова та ін. ; за заг. ред. Л. Компанцевої]. К.: НА СБУ, 2021. 500 с.
3. Основи управління інформаційною безпекою: навч. посібник / Гребенюк А.М., Рибальченко Л.В. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
4. Інформаційна безпека держави: навч. посіб. В.М.Рудницький та ін.; Черкас. держ. технол. ун-т. Харків: ДІСА ПЛЮС, 2018. 358 с.
5. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник / Львів. нац. ун-т ім. Івана Франка, Львів. шк. журналістики. Львів: ЛНУ ім. Івана Франка, 2017. 725 с.

Додаткова

6. Засоби масової комунікації як детермінанти гібридної війни: монографія / Ніколаєнко Н.О., Комарчук О.О. / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв: НУК, 2021. 217 с.
7. Вовк Н.П., Мохнар Л.І. Комунікативна складова організації та здійснення антикризового управління. Вісник Національного університету оборони України. 2021. № 1 (59). С. 63-71.
8. Костецька Т.А. Унітаризм і нова парадигма державної інформаційної політики України. Часоп. Київ. ун-ту права. 2020. № 2. С. 195–197.
9. Божкова В.В., Білан А.О. Сутність державної інформаційної політики в умовах розвитку інформаційного суспільства в Україні. Інвестиції: практика та досвід. 2019. № 11. С. 106–110.

10. Руденко О.М. Забезпечення державної безпеки України в системі захисту національних інтересів. Збірник наукових праць Донецького державного університету управління. Серія «Державне управління». 2019. Т. ХХ; Вип. 312. С. 42-50.

11. Виговська О., Бєлоусова Н. Інформаційна складова національної безпеки України: кол. монографія / Ін-т міжнар. відносин, Київ. нац. ун-т ім. Тараса Шевченка, Київ. ун-т ім. Бориса Грінченка. Київ : Київ. ун-т ім. Б. Грінченка, 2017. 166 с.

12. Карлова В. Впровадження концепції відкритого урядування в Україні як інструмент демократизації державного управління. Відкрити очі. 2017.

13. Гута С.С. Поняття «кризова ситуація, зумовлена воєнно-політичними чинниками, «воєнно-політична криза» в теорії державного управління. Інвестиції: практика та досвід. 2017. №7. С. 116-120.

14. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. Науковий вісник. Серія «Філософія». Харків: ХНПУ. 2017. Вип. 48 (частина І). С. 212–219.

15. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ : Видавничий дім «Гельветика», 2017. 168 с.

16. «Цифрова адженда України – 2020» («Цифровий порядок денний» - 2020)

Інформаційні ресурси

1. Система дистанційного навчання НУ «Чернігівська політехніка». Курс: Інституційні засади публічного управління та адміністрування https://eln.stu.cn.ua/course/view.php?id=4418

2. Законодавство України – http://www.zakon.rada.gov.ua.

3. Нормативні акти України – http://www.nau.ua

4. Офіційний сайт бібліотеки ім. В. Вернадського. – Режим доступу: http://nbuv.gov.ua/

5. Офіційний сайт Наукової бібліотеки НУ «Чернігівська політехніка». – Режим доступу: http://library2.stu.cn.ua/

6. Офіційний сайт Верховної Ради України – http://www.rada.gov.ua

7. Урядовий портал. Єдиний веб-портал органів виконавчої влади України: http://www.kmu.gov.ua