НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут економіки та менеджменту

06-07-145S

СИЛАБУС
навчальної дисципліни

SYLLABUS

Інформаційна безпека	***Information security***	
Шифр за ОП	ВВ 5.2	Code in Degree Programme
Освітній рівень: магістерський (другий)	Level of Education: Master's (second)	
Галузь знань **Культура і мистецтво**	02	Field of Knowledge: **Culture and Art**
Спеціальність **Менеджмент соціокультурної діяльності**	028	Field of Study: **Management of Sociocultural Activity**
Освітня програма **Соціальний менеджмент та інформаційна культура**	Degree Programme: **Social Management and Information Culture**	

РІВНЕ – 2024

06-07-145SСилабус навчальної дисципліни ***«Інформаційна безпека»***для здобувачів вищої освіти ступеня «магістр», які навчаються за освітньо-професійною програмою ***«Соціальний менеджмент та інформаційна культура» спеціальності 028 «Менеджмент соціокультурної діяльності» галузі знань 02 «Культура і мистецтво».***Рівне. НУВГП. 2024. 11 стор.

ОПП на сайті університету: https://ep3.nuwm.edu.ua/26595/

Розробник силабусу: *Рейнська В.Б., к.е.н., доцент кафедри філософії та культурології, доцент.*

Силабус схвалений на засіданні кафедри
Протокол № 14 від “10” червня 2024 року

Завідувач кафедри: *Шадюк Т.А., к.філос.н., доцент кафедри філософії та культурології, доцент.*

Керівник (гарант) ОП: *Шадюк Т.А., к.філос.н., доцент кафедри філософії та культурології, доцент.*

Схвалено науково-методичною радою з якості ННІ
Протокол № 14 від “10” червня 2024 року

Голова науково-методичної ради з якості ННІ: Ковшун Н.Е*., д.е.н., професор.*

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА»	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*магістр*
Освітня програма	*Соціальний менеджмент та інформаційна культура*
Спеціальність	028 *Менеджмент соціокультурної діяльності*
Рік навчання, семестр	*1 рік, 2 семестр*
Кількість кредитів	*3*
Лекції:	*16 годин денна форма навчання* *2 годин заочна форма навчання*
Практичні заняття:	*14 годин денна форма навчання* *8 годин заочна форма навчання*
Самостійна робота:	*60 годин денна форма навчання* *80 год заочна форма навчання*
Курсова робота:	*Не передбачено*
Форма навчання	*Денна/Заочна*
Форма підсумкового контролю	*залік*
Мова викладання	*українська*
ІНФОРМАЦІЯ ПРО РОЗРОБНИКА	

Лектор 	*Рейнська Вікторія Борисівна,* *кандидат економічних наук, доцент,* *кафедри філософії та культурології*
Вікіситет	http://wiki.nuwm.edu.ua/index.php/
ORCID	https://orcid.org/0000-0002-3969-2054
Як комунікувати	v.b.reinska@nuwm.edu.ua

ІНФОРМАЦІЯ ПРО ДИСЦИПЛІНУ
Мета і завдання
Мета дисципліни: формування у здобувачів вищої освіти теоретичних знань та практичних навичок щодо забезпечення інформаційної безпеки національних інтересів у будь-якій сфері життєдіяльності суспільства. *Завданням дисципліни є:* • визначення концептуальних засад, принципів, форм та методів забезпечення інформаційної безпеки; • ознайомлення з ключовими загрозами інформаційної безпеки, основами управління інформаційною безпекою; • формування навичок використання основ теорії і практики інформаційної безпеки у публічному управлінні
Посилання на розміщення освітнього компонента на навчальній платформі Moodle, на платформі освітніх програм та їхніх освітніх компонентів
https://exam.nuwm.edu.ua/course/view.php?id=6107
Передумови вивчення навчальної дисципліни
Дисципліни, що передують вивченню ОК «Цифрова безпека»: «Цифрова та інформаційна культура», «SMM та SEO технології в соціокультурній сфері». Результати вивчення дисципліни стануть у нагоді при написані кваліфікаційної роботи магістра.
Компетентності

ІК. Здатність розв’язувати складні задачі і проблеми в сфері менеджменту соціокультурної діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
ЗК1. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).
СК5. Здатність організовувати та реалізовувати науково-дослідні, науково-виробничі, соціокультурні проекти.
СК13. Здатність здійснювати аналітичну оцінку інформаційного простору соціокультурної сфери, використовувати SMM та SEO технології, а також знання з інформаційної безпеки

Програмні результати навчання (ПРН)

ПР1. Відшуковувати, аналізувати та оцінювати інформацію, необхідну для постановки і вирішення як професійних завдань, так і особистісного розвитку.
ПР5. Використовувати міждисциплінарний підхід до вирішення складних задач і проблем соціокультурної діяльності.
ПР12. Збирати необхідні дані з різних джерел, обробляти і аналізувати їх практичні результати із застосуванням сучасних методів та спеціалізованого програмного забезпечення.

Структура та зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ1. ІНФОРМАЦЙНА БЕЗПЕКА. ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тема 1. Теоретичні аспекти інформаційної безпеки
Основні поняття інформаційної безпеки управлінських систем. Інформація як товар та об'єкт безпеки

Тема 2. Поняття інформаційних загроз та їхні види
Поняття інформаційних загроз, їх види та способи впливу на об'єкт. Поняття та види комп'ютерних злочинів. Шкідливі програми для ПК і мобільних пристроїв

Тема 3. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану
Об’єкти інформаційного впливу. Доктрина інформаційної безпеки України. Центр протидії дезінформації, його функції та повноваження. «Інформаційна бульбашка» як стан інтелектуальної ізоляції. Стани людини під час перебування в «інформаційній бульбашці»

ЗМІСТОВИЙ МОДУЛЬ2. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тема 4. Підходи, принципи, методи та засоби забезпечення безпеки
Політика безпеки та її принципи. Підходи, принципи, методи та засоби забезпечення інформаційної безпеки.

Тема 5. Організація системи захисту інформації
Організаційне забезпечення інформаційної безпеки. Захист інформації в Інтернет. Захист від комп'ютерних вірусів. Етапи побудови системи захисту інформації.

Тема 6. Менеджмент та аудит систем інформаційної безпеки
Менеджмент та аудит інформаційної безпеки на рівні підприємства. Аудит інформаційної безпеки електронної комерції та комунікації. Менеджмент інформаційної безпеки електронної комерції та комунікації.

Розподіл годин за темами змістових модулів

Лекції	Год	Практичні роботи	Год	Сам. робота (год.)	Всього (год.)	Навчальні матеріали
ЗМІСТОВИЙ МОДУЛЬ1. ІНФОРМАЦІЙНА БЕЗПЕКА. ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ						
Тема 1. Теоретичні аспекти інформаційної безпеки	2	ПР-1. Інформація як товар та об'єкт безпеки	1	10	13	[3, 5, 7]
Тема 2. Поняття інформаційних загроз та їхні види	2	ПР-2. Виявлення шкідливих програм для ПК і мобільних пристроїв	1	10	13	[8, 11, 13]
Тема 3. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану	6	ПР-3. Основні завдання Центру протидії дезінформації	1	5	12	[3,6,12]
		ПР-4. Реалізація єдиної інформаційної політики в умовах воєнного стану	1	5	6	[1,4,10]
МК-1			2		2	
За змістовим модулем 1	10		6	30	46	
ЗМІСТОВИЙ МОДУЛЬ2. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ						
Тема 4. Підходи, принципи, методи та засоби забезпечення безпеки	2	ПР-5.Реалізація методів Забезпечення інформаційної безпеки	2	10	14	[3, 10, 12]
Тема 5. Організація системи захисту інформації	2	ПР-6. Алгоритми побудови системи захисту інформації	2	10	14	[4, 7, 10]
Тема 6. Менеджмент та аудит систем інформаційної безпеки	2	ПР-7. Аудит інформаційної безпеки електронної комерції та комунікації	2	10	14	[8,14,15]
МК-2			2		2	
За змістовим модулем 2	6		8	30	44	
Разом	**16**		**14**	**60**	**180**	

Відповідність програмних результатів навчання навчальним матеріалам

Теми	ПРН 1	ПРН 5	ПРН 12
Тема 1. Теоретичні аспекти інформаційної безпеки			
Тема 2. Поняття інформаційних загроз та їхні види			
Тема 3. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану			
Тема 4. Підходи, принципи, методи та засоби забезпечення безпеки			
Тема 5. Організація системи захисту інформації			

Тема 6. Менеджмент та аудит систем інформаційної безпеки			

Форми та методи навчання
Вивчення навчальної дисципліни будується на поєднанні лекцій, практичних занять, елементів дистанційного навчання, самостійної та керованої самостійної роботи студентів. Методи навчання: словесні; наочні; практичні; пояснювально-ілюстративний; репродуктивний; частково-пошуковий; дослідницький; проблемного викладу
Інструменти, обладнання, програмне забезпечення
-технічні засоби навчання: мультимедійне обладнання, ноутбук; -програмне забезпечення: програми для роботи з текстом (Microsoft Word, Google Docs) для написання конспектів та рефератів; системи пошуку нормативно-правових актів України ("ЛІГА:ЗАКОН"); програми для шифрування та захисту даних (VeraCrypt, PGP); системи управління інформаційною безпекою (ISO 27001:2013 Compliance Software); -програмне забезпечення: технології Google (Google Forms) ChatGPT; -програмне забезпечення: система дистанційного навчання Moodle.
Порядок оцінювання програмних результатів навчання

Поточний контроль здійснюється за виконанням завдань практичних робіт; за підсумками роботи під час лекційних занять.
Підсумковий контроль відбувається у вигляді проходження двох модульних контролів у формі тестування на університетській платформі MOODLE.
У тесті передбачено 32 запитання різної складності:

- рівень 1 – 24 запитання по 0,5 бала (12 балів),
- рівень 2 – 8 запитань по 0,7 бала (5,6 бала),
- рівень 3 – 2 запитання по 1,2 бала (2,4 бала).

Усього – 20 балів.

Усі форми контролю включено до 100-бальної шкали оцінювання.
За конкретні пропозиції з удосконалення змісту навчальної дисципліни студентам також можуть бути зараховані додаткові бали (до 3 балів).

Шкала оцінювання навчальних досягнень студентів

Вид заняття	Бали
1. Поточна складова оцінювання	
1.1. Практична робота 1. Інформація як товар та об'єкт безпеки.	6
1.2. Практична робота 2. Виявлення шкідливих програм для ПК і мобільних пристроїв.	9
1.3. Практична робота 3. Основні завдання Центру протидії дезінформації.	9
1.4. Практична робота 4. Реалізація єдиної інформаційної політики в умовах воєнного стану.	9
1.5. Практична робота 5. Реалізація методів Забезпечення інформаційної безпеки.	9
1.6. Практична робота 6. Алгоритми побудови системи захисту інформації.	9
1.7. Практична робота 7. Аудит інформаційної безпеки електронної комерції та комунікаціїю	9
Всього поточна складова оцінювання:	**60**
2. Модульна складова оцінювання	
2.1. Модульний контроль №1	20
2.2. Модульний контроль №2	20
Всього підсумкова складова оцінювання:	**40**
Разом:	**100**

Рекомендована література

Основна

1. Герман, М. Л. Політика та стратегія державного регулювання інформаційної безпеки. Львів: Видавництво Львівського національного університету, 2017. 275 с.
2. Гончаров, П. А. Менеджмент інформаційної безпеки: Основи та практичні аспекти. Львів: Видавництво ЛНУ ім. Івана Франка, 2020. 230 с.
3. Данилов, В. С. Інформаційна безпека в умовах сучасних загроз. Львів: Видавництво Львівської політехніки, 2018. 256 с.
4. Зубарєв, В. В. Організація системи захисту інформації: Теорія і практика. Київ: Видавництво НТУУ «КПІ», 2020. 300 с.
5. Кавун С. В. Інформаційна безпека. Навчальний посібник. Харків: Вид. ХНЕУ, 2020. 352 с.
6. Козлов, О. А. Теоретичні аспекти інформаційної безпеки. Одеса: Астропринт, 2016. 290 с.
7. Крючков, С. В. Державне регулювання у сфері інформаційної безпеки України: Проблеми та рішення. Київ: Центр учбової літератури, 2021. 220 с.
8. Кудрявцев, Ю. І. Основи інформаційної безпеки: Теорія та практика. Київ: Техніка, 2017. 320 с.
9. Лебедєв, А. С. Управління системами інформаційної безпеки. Київ: Видавничий дім «КНТ», 2022. 270 с.
10. Петренко, В. О. Інформаційна безпека України: Виклики та відповіді. Одеса: ОНУ ім. І. І. Мечникова, 2022. 240 с.
11. Романенко, О. В. Методологія та практика забезпечення інформаційної безпеки. Київ: Видавництво Національного університету «Київська політехніка», 2021. 250 с.
12. Семенов, М. І. Інформаційні загрози та їх класифікація. Харків: Національний технічний університет Харківського політехнічного інституту, 2019. 180 с.
13. Сергієнко, В. О. Підходи до забезпечення інформаційної безпеки в умовах воєнного стану. Харків: Видавництво ХНУРЕ, 2023. 260 с.
14. Тимошенко, І. В. Принципи та методи забезпечення інформаційної безпеки. Дніпро: Дніпровський національний університет імені Олеся Гончара, 2019. 245 с.
15. Черненко, А. В. Теоретичні та практичні аспекти менеджменту інформаційної безпеки. Київ: Видавництво «Міжнародні відносини», 2022. 300 с.
16. Шевченко, І. М. Аудит систем інформаційної безпеки. Київ: Видавництво «Юрінком Інтер», 2018. 210 с.

Допоміжна

17. Богуш В., Бровко В., Настрадін В. Основи кіберпростору, кіберзахисту та кібербезпеки. Видавництво: Ліра-К., 2021. 554 с.
18. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань»: монографія. Київ-Одеса : Фенікс, 2021. 176 с.
19. Інтеграція цифрових технологій в освітній процес: виклики та перспективи: монографія / Саєнко Н.С., Голуб Т.П., Лавриш Ю.Е., Лук'яненко В.В., Литовченко І.М. Видавництво: Центр навчальної літератури, 2022. 220 с.
20. Кулініч О.О. Охорона та захист прав інтелектуальної власності: економіко-правові підходи. Видавництво «Ліра-К», 2019. 276 с.
21. Ланде Д.В., Правові питання конкурентної розвідки. Інформація і право. 2020. 2(33). С. 51-68. DOI: https://doi.org/10.37750/2616-6798.2020.2(33).208089
22. Росс А. Індустрії майбутнього. Видавництво «Наш Формат», 2022. 320 с.
23. Роуз Д. Цифровий брендинг. Видавництво «Фабула», 2020. 256 с.
24. Скіннер К. Людина цифрова. Видавництво «Фабула», 2020. 272 с.

Інформаційні ресурси в Інтернет

25. Національний центр кібербезпеки України. Теоретичні аспекти інформаційної безпеки : веб-сайт. URL: https://ncc.gov.ua/ (дата звернення: 01.09.2024).
26. Інститут інформаційної безпеки. Теоретичні основи інформаційної безпеки : веб-сайт. URL: [https://iis.org.ua/theory-information-security] (https://iis.org.ua/theory-information-security) (дата звернення: 01.09.2024).
27. Міністерство цифрової трансформації України. Захист інформаційних систем : веб-сайт. URL: https://thedigital.gov.ua/ (дата звернення: 01.09.2024).
28. Ukrainian Cyber Security Group. Поняття інформаційних загроз : веб-сайт. URL: https://ucsg.org.ua/ (дата звернення: 01.09.2024).
29. Центр моніторингу та захисту інформації. Підходи до забезпечення інформаційної безпеки : веб-сайт. URL: [https://cmpi.gov.ua/] (https://cmpi.gov.ua/) (дата звернення: 01.09.2024).
30. Методи забезпечення інформаційної безпеки. Інтернет-ресурс. URL: https://it-ukraine.org.ua/methods-information-security (дата звернення: 01.09.2024).
31. CyberSecurity in Ukraine. Державне регулювання в умовах воєнного стану : веб-сайт. URL: https://cybersecurity.com.ua/ (дата звернення: 01.09.2024).
32. Аудит і безпека інформації. Основи аудиту систем інформаційної безпеки : веб-сайт. URL: https://auditinfosec.com.ua/ (дата звернення: 01.09.2024).
33. Інститут безпеки та захисту інформації. Організація системи захисту інформації : веб-сайт. URL: https://ibzi.org.ua/ (дата звернення: 01.09.2024).
34. Кібербезпека України. Принципи і методи забезпечення інформаційної безпеки : веб-сайт. URL: [https://cybersecurity.gov.ua/] (https://cybersecurity.gov.ua/) (дата звернення: 01.09.2024).
35. Центр інформаційної безпеки. Поняття інформаційних загроз : веб-сайт. URL: https://cib.org.ua/ (дата звернення: 01.09.2024).
36. Управління інформаційною безпекою в Україні. Управління та менеджмент систем інформаційної безпеки : веб-сайт. URL: [https://info-security.ua/] (https://info-security.ua/) (дата звернення: 01.09.2024).
37. Безпека даних та інформації. Підходи та засоби захисту інформації : веб-сайт. URL: https://datasecurity.com.ua/ (дата звернення: 01.09.2024).
38. Безпека інформаційних систем в Україні. Принципи забезпечення безпеки : веб-сайт. URL: https://securitysys.org.ua/ (дата звернення: 01.09.2024).
39. Проблеми та рішення в інформаційній безпеці. Менеджмент і аудит систем інформаційної безпеки : веб-сайт. URL: [https://info-problems.com.ua/] (https://info-problems.com.ua/) (дата звернення: 01.09.2024).

Поєднання навчання та досліджень

Здобувачі мають можливість додатково отримати бали за виконання індивідуальних завдань дослідницького характеру, можуть бути долучені до написання та опублікування наукових статей з тематики навчальної дисципліни, участі в науково-практичних конференціях відповідного спрямування.

ПОЛІТИКИ ВИКЛАДАННЯ ТА НАВЧАННЯ

Перелік соціальних, «м’яких» навичок (soft skills)

Взаємодія з інформаційними технологіями. Аналітичні навички. Інформаційна грамотність. Здатність до навчання. Здатність логічно обґрунтовувати позицію, оцінювати ризики та приймати рішення.

Дедлайни та перескладання

Поточні терміни захисту практичних робіт становлять два тижні після проведення заняття. Крайні терміни захисту практичн робіт регламентується останнім тижнем перед початком екзаменаційної сесії. У разі невиконання студентом вимог щодо поточного оцінювання протягом семестру (невчасне виконання) завдання) оцінку може бути знижено в межах 10%.
Ліквідація академічної заборгованості здійснюється згідно з «Порядком ліквідації академічних заборгованостей у НУВГП», http://ep3.nuwm.edu.ua/4273/. За цим документом реалізується право студента на повторне проходження навчальної практики. Оголошення стосовно дедлайнів здачі та перездачі оприлюднюються на сторінці MOODLE https://exam.nuwm.edu.ua/course/view.php?id=2714

Неформальна та інформальна освіта

Студенти мають право на перезарахування результатів навчання,
*набутих у неформальній та інформальній освіті (http://nuwm.edu.ua/sp/neformalna-osvita). Студенти можуть самостійно на платформах Prometheus, Coursera, edEx, edEra, Future Learn опановувати матеріал для перезарахування результатів навчання (*https://prometheus.org.ua/course/course-v1:Prometheus+DSPL101+2023_T1*). При цьому важливо, щоб знання та навички, що формуються під час проходження певного онлайн-курсу чи його частин, мали зв'язок з очікуваними програмними результатами навчальної дисципліни та перевірялись в підсумковому оцінюванні.*

Перед початком проходження обраних курсів необхідно отримати згоду викладача.

Правила академічної доброчесності

У разі виявлення копіювання результатів виконання завдань студенту завдання не зараховується. Студент повторно отримує завдання і виконує його самостійно.
Документи стосовно академічної доброчесності (про плагіат, порядок здачі звіту, кодекс честі студентів, документи Національного агентства стосовно доброчесності) наведені на сторінці НУВГП http://nuwm.edu.ua/sp/akademichna-dobrochesnisti

Вимоги до відвідування

- *Заняття відбуваються згідно розкладу https://desk.nuwm.edu.ua/cgi-bin/timetable.cgiофлайн або онлайн за допомогою Google Meet за лінком: https://meet.google.com/*
- *Консультації проводяться за потреби в режимі онлайн за допомогою Google Meet у домовлений час зі студентами.*
- *Здобувачі можуть на заняттях використовувати мобільні телефони та ноутбуки, але виключно в навчальних цілях.*
- *Студенту не дозволяється пропускати заняття без поважних причин.*
- *За наявності об'єктивних причин пропуску занять, студенти можуть самостійно ознайомитися з теоретичним матеріалом на платформі MOODLE https://exam.nuwm.edu.ua/course/view.php?id=4271*

ЛекторРейнська Вікторія Борисівна, к.е.н., доцент, доцент кафедри філософії та культурології

Автор
Доцент кафедри комп'ютерних технологій
та економічної кібернетики — Вікторія РЕЙНСЬКА

Затверджено

Проректор з науково-педагогічної та
навчальної роботи — Валерій СОРОКА

документ підписаний КЕП
Номер документа СИЛ №944
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 3FAA9288358EC003040000009B6C3700C8C2C100