НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут економіки та менеджменту

06-07-72S

СИЛАБУС
навчальної дисципліни

SYLLABUS

Цифрова безпека		Digital Security
Шифр за ОП	ВБ 1.1	Code in Educational Program
Освітній рівень: бакалаврський (перший)		Educational level: Bachelor's (first)
Галузь знань: Гуманітарні науки	03	Field of knowledge: Humanities
Спеціальність: **Культурологія**	034	Field of study: **Cultural Studies**
Освітня програма: **Креативна та цифрова культура**		Educational Program: **Creative and digital culture**

РІВНЕ - 2023

Силабус навчальної дисципліни Цифрова безпека для здобувачів вищої освіти ступеня «бакалавр», які навчаються за освітньо-професійною програмою ID 35948 Креативна та цифрова культура, спеціальності 034 Культурологія. Рівне. НУВГП. 2023. 12 стор.

ОПП на сайті університету: https://ep3.nuwm.edu.ua/21004/

Розробник силабусу: Рейнська В.Б., кандидат економічних наук, доцент, доцент кафедри філософії та культурології

Силабус схвалений на засіданні кафедри філософії та культурології Протокол № 5 від "22" листопада 2023 року

Завідувач кафедри: Шадюк Т.А., кандидат філософських наук, доцент.

Керівник ОПП: Коберська Т.А., кандидат філософських наук, доцент.

Схвалено науково-методичною радою з якості ННІ ЕМ
Протокол № 6 від “30” листопада 2023 року

Голова науково-методичної ради з якості ННІ АКОТ: Н.Е. Ковшун, доктор економічних наук, професор

Попередня версія силабусу 06-07-17S

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Цифрова безпека»	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*бакалавр*
Освітня програма	ID 35948 Креативна та цифрова культура
Спеціальність	034 Культурологія
Рік навчання, семестр	*3 рік, 1 семестр*
Кількість кредитів	*6*
Лекції:	*30 год*
Практичні заняття:	*30 год*
Самостійна робота:	*120 год*
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, доцент кафедри комп’ютерних технологій та економічної кібернетики*
Вікіситет	http://wiki.nuwm.edu.ua/index.php/Рейнська_Вікторія_Борисівна
ORCID	https://orcid.org/0000-0002-3969-2054
Як комунікувати	v.b.reinska@nuwm.edu.ua

ІНФОРМАЦІЯ ПРО ДИСЦИПЛІНУ

Мета і завдання

Мета дисципліни: оволодіння здобувачами вищої освіти компетенцій для класифікації та характеристики складових цифрової безпеки та захисту інформації.
Завданням дисципліни є:

- *ознайомити студентів сучасними програмно-технічними засобами забезпечення цифрової безпеки;*
- *сформувати здатність виявляти основні загрози цифрової безпеки;*
- *сформувати уміння встановлювати та налаштовувати типові програмні засоби захисту інформації;*
- *навчити аналізувати і використовувати типові криптографічні засоби та методи захисту інформації, у тому числі електронний цифровий підпис.*
- *сформувати уміння забезпечувати антивірусний захист.*

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=2714

Передумови вивчення навчальної дисципліни

Дисципліни, що передують вивченню дисципліни «Цифрова безпека»: "Основи цифрових технологій".
Результати вивчення дисципліни стануть у нагоді при вивченні «SMM технології».

Компетентності

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми.
ЗК 12. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
ФК 5. Здатність використовувати різноманітні джерела інформації та методологічний апарат культурології для виявлення, аналізу культурних потреб суспільства.
ФК 10. Здатність популяризувати знання про культуру та поширювати інформацію культурологічного змісту, використовуючи сучасні інформаційні, комунікативні засоби та візуальні технології.
ФК 14. Здатність надавати аналітичну оцінку інформаційного простору, використовувати SMM технології та знання з інформаційної безпеки з урахуванням особливостей перебігу соціокультурних і політичних процесів.
ФК 15. Здатність до особистісного та професійного самовдосконалення, навчання та саморозвитку.

Програмні результати навчання (ПРН)

ПРН 5. Збирати, упорядковувати та аналізувати інформацію щодо культурних явищ, подій та історико-культурних процесів.
ПРН 6. Виявляти, перевіряти та узагальнювати інформацію щодо різноманітних контекстів культурної практики, визначати ступінь її актуальності із застосуванням релевантних джерел, інформаційних, комунікативних засобів та візуальних технологій.
ПРН 17. Здійснювати WEB-аналітику у сфері сучасних інформаційних технологій з проблем культури та оцінювати ефективність SMM технологій.
ПРН 18. Продемонструвати вправність у володінні комп'ютерними технологіями, включаючи спеціальну термінологію, для проведення пошуку спеціалізованої інформації, вивчення документації, коментування програмного забезпечення.
ПРН 19. Визначати інформаційні властивості повідомлення ЗМІ, що стосуються культури, культурної спадщини та міжкультурних комунікацій.

Структура та зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1.
ЦИФРОВА БЕЗПЕКА. КОМП'ЮТЕРНІ ВІРУСИ ТА ЗАХИСТ ВІД НИХ

Тема 1. Поняття "цифрова безпека". Складові цифрової безпеки.
Проблема цифрової безпеки суспільства. Визначення поняття "цифрова безпека". Доступність інформації. Цілісність інформації .Конфіденційність інформації

Тема 2. Система формування режиму цифрової безпеки. Класифікація загроз " цифрової безпеки".
Завдання цифрової безпеки суспільства. Рівні формування режиму цифрової безпеки. Цілі, завдання та зміст адміністративного рівня. Розроблення політики цифрової безпеки.
Класи загроз цифрової безпеки. Канали несанкціонованого доступу до інформації.

Тема 3. Віруси як загроза цифровій безпеці. Класифікація комп'ютерних вірусів.
Комп'ютерні віруси та цифрова безпека. Характерні риси комп'ютерних вірусів. Класифікація комп'ютерних вірусів за середовищем існування. Класифікація комп'ютерних вірусів за особливостями алгоритму роботи. Класифікація комп'ютерних вірусів за деструктивними можливостями.

Тема 4. Характеристика "вірусоподібних" програм. Антивірусні програми.
Види "вірусоподібних" програм. Характеристика "вірусоподібних" програм. Утиліти прихованого адміністрування. "Intended"-віруси. Особливості роботи антивірусних програм. Класифікація антивірусних програм. Фактори, що визначають якість антивірусних програм.

Тема 5. Профілактика комп'ютерних вірусів. Виявлення невідомого вірусу.
Характеристика шляхів проникнення вірусів у комп'ютери. Правила захисту від комп'ютерних вірусів. Виявлення завантажувального вірусу. Виявлення резидентного вірусу. Виявлення макровірусу. Загальний алгоритм виявлення вірусу

ЗМІСТОВИЙ МОДУЛЬ 2.
МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Тема 6 Особливості забезпечення цифрової безпеки в комп'ютерних мережах.
Особливості інформаційної безпеки в комп'ютерних мережах. Специфіка засобів захисту в комп'ютерних мережах.

Тема 7. Мережеві моделі передачі даних.Адресація в глобальних мережах
Поняття протоколу передачі даних. Принципи організації обміну даними в обчислювальних мережах. Транспортний протокол TCP і модель TCP/IP.Основи IP-протоколу. Класи адрес обчислювальних мереж. Система доменних імен.

Тема 8. Класифікація віддалених загроз в обчислювальних мережах. Типові віддалені атаки та їх характеристика.
Класи віддалених загроз та їхня характеристика. Віддалена атака "аналіз мережевого трафіку". Віддалена атака "підміна довіреного об'єкта". Віддалена

атака "хибний об'єкт". Віддалена атака "відмова в обслуговуванні".

Тема 9. Принципи захисту розподілених обчислювальних мереж.

Причини успішної реалізації віддалених загроз в обчислювальних мережах. Принципи побудови захищених обчислювальних мереж

Тема 10. Ідентифікація та автентифікація. Методи розмежування доступу.

Визначення понять "ідентифікація" та "автентифікація". Механізм ідентифікації та автентифікації користувачів. Методи розмежування доступу. Мандатне та дискретне керування доступом

Тема 11. Криптографія та шифрування.

Структура криптосистеми. Класифікація систем шифрування даних. Симетричні та асиметричні методи шифрування. Механізм електронного цифрового підпису.

Тема 12. Реєстрація та аудит. Міжмережеве екранування.

Визначення та зміст реєстрації та аудиту інформаційних систем. Етапи реєстрації та методи аудиту подій інформаційної системи. Класифікація міжмережевих екранів. Характеристика міжмережевих екранів.

Тема 13. Технологія віртуальних приватних мереж (VPN)

Сутність і зміст технології віртуальних приватних мереж. Поняття "тунелю" під час передавання даних у мережах.

Розподіл годин за темами змістових модулів

Лекції	Год	Практичні роботи	Год	Сам. робота (год.)	Всього (год.)	Навчальні матеріали
ЗМІСТОВИЙ МОДУЛЬ 1. ЦИФРОВА БЕЗПЕКА. КОМП'ЮТЕРНІ ВІРУСИ ТА ЗАХИСТ ВІД НИХ						
Тема 1. Поняття "цифрова безпека". Складові цифрової безпеки.	2	ПР-1. Аналіз прикладів порушення цифрової безпеки. Виявлення складових цифрової безпеки та характеристик інформаційної системи в конкретних ситуаціях.	2	5	9	[1, 2]
Тема 2. Система формування режиму цифрової безпеки. Класифікація загроз " цифрової безпеки".	2	ПР-2. Виявлення загроз цифрової безпеки в конкретних ситуаціях.	2	5	9	[2, 3, 6]
Тема 3. Віруси як загроза цифровій безпеці. Класифікація комп'ютерних вірусів.	2	ПР-3. Виявлення функціональних можливостей та принципів роботи троянської програми на прикладі клавіатурного шпигуна.	2	10	14	[1, 2, 5]
Тема 4. Характеристика "вірусоподібних" програм. Антивірусні програми.	4	ПР-4. Встановлення антивірусного програмного забезпечення.	2	10	16	[1, 2, 3, 6]
Тема 5. Профілактика комп'ютерних вірусів. Виявлення невідомого вірусу.	2	ПР-5. Виконання перевірки комп’ютера на наявність ознак зараження шкідливим програмним забезпеченням.	2	10	14	[1, 2, 5]

МК-1	-		2		2	
За змістовим модулем 1	12		12	40	64	
ЗМІСТОВИЙ МОДУЛЬ 2. МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ						
Тема 6 Особливості забезпечення цифрової безпеки в комп'ютерних мережах.	2	ПР-6. Створення користувачів та груп в операційній системі Windows. Розв'язання завдань пошуку та скидання паролів користувачів.	2	10	14	[1, 2, 3, 6]
Тема 7. Мережеві моделі передачі даних. Адресація в глобальних мережах	2	ПР-7. Виконання налаштування системи парольного захисту в локальній системі безпеки операційної системи Windows.	2	10	14	[1, 3, 6]
Тема 8. Класифікація віддалених загроз в обчислювальних мережах. Типові віддалені атаки та їх характеристика.	2	ПР-8. Класифікація віддалених загроз в обчислювальних мережах. Типові віддалені атаки та їх характеристика.	2	10	14	[1, 2, 4, 5]
Тема 9. Принципи захисту розподілених обчислювальних мереж.	2	ПР-9. Виконання встановлення програмного забезпечення для стенографічного перетворення. Виконання операцій зі створення та обміну прихованою інформацією.	2	10	14	[1, 2, 4, 6]
Тема 10. Ідентифікація та автентифікація. Методи розмежування доступу.	2	ПР-10. Виконання операцій з обміну відкритими ключами через інфраструктуру відкритих ключів, відправці та отриманню зашифрованих та підписаних ЕЦП документів.	2	10	14	[1, 2, 3, 5]
Тема 11. Криптографія та шифрування.	2	ПР-11. Виконання встановлення програмного забезпечення для роботи з інфраструктурою відкритого ключа. Створення відкритого та закритого криптографічного ключа.	2	10	14	[1, 9, 11]
Тема 12. Реєстрація та аудит. Міжмережеве екранування.	4	ПР-12.Виконання налаштування міжмережевого екрану: створення правил фільтрації пакетів для запобігання доступу до внутрішніх сервісів.	2	10	16	[2, 5, 9]
Тема 13. Технологія	2	ПР-13. Технологія	2	10	14	[1, 3, 11]

віртуальних приватних мереж (VPN)		віртуальних приватних мереж (VPN)				
МК-2	0		2		2	
За змістовим модулем 2	18		18	80	116	
Разом	**30**		**30**	**120**	**180**	

Відповідність програмних результатів навчання навчальним матеріалам

Теми	ПРН 1	ПРН 18
Тема 1. Поняття "цифрова безпека". Складові цифрової безпеки.		
Тема 2. Система формування режиму цифрової безпеки. Класифікація загроз " цифрової безпеки".		
Тема 3. Віруси як загроза цифровій безпеці. Класифікація комп'ютерних вірусів.		
Тема 4. Характеристика "вірусоподібних" програм. Антивірусні програми.		
Тема 5. Профілактика комп'ютерних вірусів. Виявлення невідомого вірусу.		
Тема 6 Особливості забезпечення цифрової безпеки в комп'ютерних мережах.		
Тема 7. Мережеві моделі передачі даних.Адресація в глобальних мережах		
Тема 8. Класифікація віддалених загроз в обчислювальних мережах. Типові віддалені атаки та їх характеристика.		
Тема 9. Принципи захисту розподілених обчислювальних мереж.		
Тема 10. Ідентифікація та автентифікація. Методи розмежування доступу.		
Тема 11. Криптографія та шифрування.		
Тема 12. Реєстрація та аудит. Міжмережеве екранування.		
Тема 13. Технологія віртуальних приватних мереж (VPN)		

Форми та методи навчання

Вивчення навчальної дисципліни будується на поєднанні лекцій, лабораторних занять, елементів дистанційного навчання, самостійної та керованої самостійної роботи студентів.
Методи навчання: інформаційно-ілюстративний, презентації, тренінги, обговорення, ситуаційні дослідження, командна робота.

Інструменти, обладнання, програмне забезпечення

-технічні засоби навчання: мультимедійне обладнання, ноутбук;
-програмне забезпечення: MS Windows, доступ до Інтернет;
-програмне забезпечення: технології Google (Google Forms) ChatGPT.
-програмне забезпечення: система дистанційного навчання Moodle.

Порядок оцінювання програмних результатів навчання

Поточний контроль здійснюється за виконанням завдань лабораторних 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. Аналіз прикладів порушення цифрової безпеки. Виявлення складових цифрової безпеки та характеристик інформаційної системи в конкретних ситуаціях.	4
1.2. Практична робота 2. Виявлення загроз цифрової безпеки в конкретних ситуаціях.	4
1.3. Практична робота 3. Виявлення функціональних можливостей та принципів роботи троянської програми на прикладі клавіатурного шпигуна.	4
1.4. Практична робота 4. Встановлення антивірусного програмного забезпечення.	4
1.5. Практична робота 5. Виконання перевірки комп'ютера на наявність ознак зараження шкідливим програмним забезпеченням.	4
1.6. Практична робота 6. Створення користувачів та груп в операційній системі Windows. Розв'язання завдань пошуку та скидання паролів користувачів.	5
1.7. Практична робота 7. Виконання налаштування системи парольного захисту в локальній системі безпеки операційної системи Windows	5
1.8. Практична робота 8. Класифікація віддалених загроз в обчислювальних мережах. Типові віддалені атаки та їх характеристика.	5
1.9. Практична робота 9. Виконання встановлення програмного забезпечення для стенографічного перетворення. Виконання операцій зі створення та обміну прихованою інформацією.	5
1.10. Практична робота 10. Виконання операцій з обміну відкритими ключами через інфраструктуру відкритих ключів, відправці та отриманню зашифрованих та підписаних ЕЦП документів.	5
1.11. Практична робота 11. Виконання встановлення програмного забезпечення для роботи з інфраструктурою відкритого ключа. Створення відкритого та закритого криптографічного ключа.	5
1.12. Практична робота 12. Виконання налаштування міжмережевого екрану: створення правил фільтрації пакетів для запобігання доступу до внутрішніх сервісів.	5
1.13. Практична робота 13. Технологія віртуальних приватних мереж (VPN)	5
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. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.

2. Кавун С. В. Інформаційна безпека. Навчальний посібник. Харків: Вид. ХНЕУ, 2020. 352 с.
3. Когут Ю. Кібервійни, кібертероризм, кіберзлочинність. Видавництво: Дакор, Консалтингова компанія Сідкон, 2022. 284 с.
4. Когут Ю. Корпоративна безпека: практичний посібник. Видавництво: Дакор, Консалтингова компанія Сідкон, 2021. 460 с.
5. Методи та засоби захисту інформації : навчальний посібник / В.А. Лахно, Є. В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. К. : ЦП «Компринт» О.В., 2020. 444 с.
6. Мистецтво залишатися непоміченим. Хто ще читає ваші мейли / пер. з анг. О. Асташова. К.: Наш Формат, 2019. 280 с.
7. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник, 2018. К., 2018, 105 с. (Електронна версія http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne)

Допоміжна

8. Андрощук Г. Глобальні стандарти етики штучного інтелекту. Інтелектуальна власність. 2021. № 11. С. 34-41.
9. Богуш В., Бровко В., Настрадін В. Основи кіберпростору, кіберзахисту та кібербезпеки. Видавництво: Ліра-К., 2021. 554 с.
10. Гупта С. Цифрова стратегія. Посібник для переосмислення бізнесу. Видавництво «КМ-БУКС», 2020. 320 с.
11. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань»: монографія. Київ-Одеса : Фенікс, 2021. 176 с.
12. Зянько В.В. Раціоналізація бізнесової поведінки підприємств України шляхом аналізу переваг танебезпек конкурентної розвідки та промислового шпигунства. Причорноморські економічні студії. 2016. Вип. 6. С. 187-191
13. 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.
14. Кулініч О.О. Охорона та захист прав інтелектуальної власності: економіко-правові підходи. Видавництво «Ліра-К», 2019. 276 с.
15. 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
16. Матюшко В.І. Аналітичне дослідження. Широкосмуговий доступ до Інтернету в Україні: стан та перспективи. - Intel, 2012, 146 с.
17. Росс А. Індустрії майбутнього. Видавництво «Наш Формат», 2022. 320 с.
18. Роуз Д. Цифровий брендинг. Видавництво «Фабула», 2020. 256 с.
19. Скіннер К. Людина цифрова. Видавництво «Фабула», 2020. 272 с.

Інформаційні ресурси в Інтернет

20. Всесвітня організація інтелектуальної власності (ВОІВ). Режим доступу: https://www.wipo.int/portal/en/index.html
21. Закон України «Про захист персональних даних» https://zakon.rada.gov.ua/laws/show/2297-17#Text
22. Міністерство інфраструктури України. https://mtu.gov.ua/
23. Міністерство та Комітет цифрової трансформації України. https://thedigital.gov.ua/ Міністерство фінансів України. https://www.mof.gov.ua/uk
24. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник, 2018. /За ред. О.В.Лісового та ін.-К., 2018, - 105 с. http://isearch.kiev.ua/uk/book/1954-445000-informationsecurity-when-browsing-the-interne)
25. Науковий журнал «Цифрова платформа: інформаційні технології в соціокультурній сфері». Режим доступу: http://infotech-soccult.knukim.edu.ua/
26. Національна бібліотека України ім. В. І. Вернадського. Режим доступу: http://www.nbuv.gov.ua/ Український інститут науково-технічної експертизи та інформації. Режим доступу: http://www.uintei.kiev.ua/
27. Офіційний портал Верховної Ради України. Режим доступу https://www.rada.gov.ua/

28. Про доступ до публічної інформації: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text
29. Про електронні документи та електронний документообіг: Закон України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
30. Про електронну комерцію: Закон України. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text
31. Про захист інформації в інформаційно-комунікаційних системах: Закон України. URL: https://zakon.rada.gov.ua/laws/show/80/94- 6 %D0%B2%D1%80#Text
32. Про інформацію: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
33. Про основні засади забезпечення кібербезпеки України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
34. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
35. Стратегія інформаційної безпеки – 2025 https://dslua.org/publications/stratehiia-informatsiynoi-bezpeky-2025- shcho-zminytsia-u-sferi-tsyfrovykh-prav/

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 педагогічного 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-dobrochesnistj*
Вимоги до відвідування
• *Заняття відбуваються згідно розкладу https://desk.nuwm.edu.ua/cgi-bin/timetable.cgi офлайн 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*

Лектор Рейнська 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 №225
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 58E2D9E7F900307B04000000807E2D0054327D00