НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ

Навчально-науковий інститут економіки та менеджменту

06-14-244S

СИЛАБУС навчальної дисципліни **SYLLABUS**	**Інформаційна безпека** **Informational security**	
Шифр за ОП Code in Degree Programme	ФП15	
Освітній рівень Level of Education	бакалаврський (перший) Bachelor`s (first)	
Галузь знань Field of Knowledge	02	Культура і мистецтво Culture and arts
Спеціальність Field of Study	029	Інформаційна, бібліотечна та архівна справа Information, library and archival studies
Освітня програма Degree Programme	Управління інформаційними комунікаціями Information Communication Management	

м. Рівне – 2023

Силабус навчальної дисципліни «Інформаційна безпека» для здобувачів вищої освіти ступеня «бакалавр», які навчаються за освітньо-професійною програмою «Управління інформаційними комунікаціями» спеціальності 029 «Інформаційна, бібліотечна та архівна справа». Рівне. НУВГП. 2023. 10 стор.

ОПП на сайті університету:
https://is.gd/Qbmkfj

Розробник силабусу:
Маланчук Л.О.,к.е.н., доцент кафедри публічного управління, адміністрування та інформаційної діяльності

Силабус схвалений на засіданні кафедри
Протокол № 8 від 26 січня 2023 року.

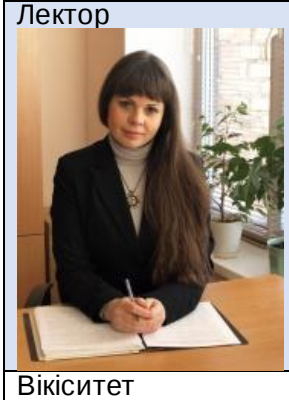
Завідувач кафедри публічного управління, адміністрування та інформаційної діяльності:
Тихончук Л.Х., д.н з держ упр., доцент.

Керівник (гарант) освітньої програми:
Цецик Я. П., к.і.н., доцент кафедри публічного управління, адміністрування та інформаційної діяльності

Схвалено науково-методичною радою з якості ННІЕМ
Протокол № 5 від 21 лютого 2023 року

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

Попередня версія силабусу - 06-14-147S

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ІНФОРМАЦІЙНА БЕЗПЕКА	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	Бакалавр
Освітня програма	Управління інформаційними комунікаціями
Спеціальність	029 «Інформаційна, бібліотечна та архівна справа»
Рік навчання, семестр	3 рік, 5 семестр
Кількість кредитів	3 кредити
Лекції:	16 годин денна форма навчання
Практичні заняття:	14 годин денна форма навчання
Самостійна робота	60 годин денна форма навчання
Курсова робота:	-
Форма навчання	*Денна*
Форма підсумкового контролю	Екзамен
Мова викладання	Державна
ІНФОРМАЦІЯ ПРО РОЗРОБНИКА (ІВ)	
ПРОФАЙЛ ЛЕКТОРІВ	
Лектор 	Маланчук Лариса Олексіївна к.е.н., доцент кафедри публічного управління, адміністрування та інформаційної діяльності
Вікіситет	*URL*: *http://wiki.nuwm.edu.ua/index.php/%D0%A4%D0%B0%D0%B9%D0%BB:1744.jpg*
ORCID	URL: *https://orcid.org/0000-0002-6341-5639*
Канали комунікації	E-mail: l.o.malanchuk@nuwm.edu.ua
ІНФОРМАЦІЯ ПРО НАВЧАЛЬНУ ДИСЦИПЛІНУ	
Мета та завдання	
Навчальна дисципліна «Інформаційна безпека» є нормативною і входить до циклу дисциплін професійної та практичної підготовки бакалаврів за спеціальністю *029 Інформаційна, бібліотечна та архівна справа* Метою викладання навчальної дисципліни «Основи інформаційної безпеки» є формування знань, умінь і навичок у студентів щодо основних понять, принципів і засобів забезпечення особистої інформаційної безпеки та безпеки в інформаційних системах на підприємствах, організаціях та установах	
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=4389	
Передумови вивчення* (місце освітнього компоненту в структурно-логічній схемі)	
Для опанування даного ОК здобувачам необхідні знання із таких ОК: ЗП11 Системи управління базами даних, ФП4 «Документно-інформаційні комунікації». Отримані знання та компетентності здобувачі можуть використати під час вивчення ОК: ФП16 Зв'язки з громадськістю.	
Компетентності	
Вивчення навчальної дисципліни надає здобувачам вищої освіти компетентностей щодо: ЗК6. Навички використання інформаційних і комунікативних технологій. ЗК7. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел. ФК1. Здатність здійснювати відбір, аналіз, оцінку, систематизацію, моніторинг, організацію, зберігання, розповсюдження та надання в користування інформації та знань у будь-яких форматах. ФК3. Здатність використовувати сучасні прикладні комп'ютерні технології, програмне забезпечення, мережеві та мобільні технології для вирішення професійних завдань. ФК10. Здатність адмініструвати соціальні мережі, електронні бібліотеки та архіви.	

ФК17. Здатність здійснювати захист інформації на різних типах носіїв.

Програмні результати навчання (РН)*

Результатами навчання, які набувають здобувачі вищої освіти вивчаючи дану дисципліну є:

РН1. Знати і розуміти наукові засади організації, модернізації та впровадження новітніх технологій в інформаційній, бібліотечній та архівній діяльності.

РН4. Застосовувати у професійній діяльності технології інформаційного менеджменту, створення і підтримки функціонування електронних бібліотек та архівів, методологію вивчення та задоволення культурних та інформаційних потреб користувачів.

РН9.Оцінювати можливості застосування новітніх інформаційно-комп'ютерних та комунікаційних технологій для вдосконалення практик виробництва інформаційних продуктів і послуг.

РН12. Застосовувати сучасні методики і технології автоматизованого опрацювання інформації, формування та використання електронних інформаційних ресурсів та сервісів.

РН19. Дотримуватися і реалізовувати основні засади охорони праці та безпеки життєдіяльності.

РН21. Кваліфіковано захищати й використовувати інформацію в умовах загроз та інформаційних протистоянь.

Структура та зміст освітнього компонента

*Тема 1. Поняття інформаційної безпеки (*Основні задачі інформаційної безпеки. Важливість і складність проблеми інформаційної безпеки. Інформація, що підлягає захисту. Державна таємниця. Сфери розповсюдження державної таємниці на інформацію. Комерційна таємниця. Персональні дані.*)* (РН12, РН21)*;*

*Тема 2. Загрози інформаційної безпеки (*Основні загрози доступності. Основні загрози цілісності. Основні загрози конфіденційності. Шкідливе програмне забезпечення. Перехоплення даних та канали витоку інформації.*)* (РН9, РН4, РН21)*;*

*Тема 3. Порушники інформаційної безпеки (*Модель поведінки потенційного порушника. Класифікація порушників. Методика вторгнення. Дії, що призводять до неправомірного оволодіння конфіденційною інформацією. Умови, що сприяють неправомірному оволодінню конфіденційною інформацією*)* (РН17, РН19)*;*

*Тема 4. Огляд законодавства в галузі інформаційної безпеки (*Основні поняття законодавчого рівня інформаційної безпеки. Система забезпечення інформаційної безпеки України. Нормативно-правові документи. Форми правового захисту інформації. Українське законодавство в галузі інформаційної безпеки. Зарубіжне законодавство в галузі інформаційної безпеки.*)* (РН1, РН9, РН19)*;*

*Тема 5. Огляд міжнародних стандартів у галузі інформаційної безпеки (*Стандарти і специфікації в галузі безпеки інформаційних систем. «Помаранчева книга» як оцінний стандарт. Класи безпеки інформаційних систем. Технічна специфікація X.800 Стандарт ISO/IEC 15408. Розвиток стандартів з управління ризиками. Стандарт ISO/IEC TR 13335*) (РН6, РН13, РН16, РН19);*

*Тема 6. Адміністративний рівень інформаційної безпеки (*Поняття політики безпеки. Розробка політики безпеки. Програма реалізації політики безпеки. Синхронізація програми безпеки з життєвим циклом систем. Управління ризиками. Змістовий модуль №3 Організаційний та технічний рівні інформаційної безпеки.*)* (РН6, РН13, РН16, РН19)*;*

*Тема 7. Основні класи заходів організаційного рівня (*Основні класи заходів організаційного рівня. Управління персоналом. Фізичний захист. Заходи щодо захисту локального комп'ютера з конфіденційною інформацією. Підтримка роботоздатності. Реагування на порушення режиму безпеки. Планування відновлювальних робіт.*)* (РН6, РН13, РН16, РН19);

*Тема 8. Фізичні засоби захисту (*Поняття інженерно-технічного захисту. Фізичні засоби захисту. Охоронні системи. Охоронне телебачення. Охоронне освітлення та засоби охоронної сигналізації. Захист елементів будинків і приміщень. Апаратні та програмні засоби захисту.*)* (РН6, РН13, РН16, РН19);

*Тема 9. Криптографічні засоби захисту (*Основні поняття криптографії. Методи шифрування. Криптографічні протоколи. Контроль цілісності. Технологія шифрування мови. Стеганографічні засоби захисту Змістовий модуль №4 Система забезпечення інформаційної безпеки.*)* (РН6, РН13, РН16, РН19);

*Тема 10. Особливості сучасних інформаційних систем з погляду безпеки (*Особливості сучасних інформаційних систем з погляду безпеки. Основні сервіси безпеки. Принципи архітектурної безпеки.*)* (РН6, РН13, РН16, РН19);

*Тема 11. Основні сервіси безпеки. Екранування (*Аналіз захищеності. Забезпечення високої доступності. Тунелювання. Управління інформаційними системами. Екранування. Аналіз захищеності. Забезпечення високої доступності.*)* (РН6, РН13, РН16, РН19);

*Тема 12. Система забезпечення інформаційної безпеки (*Основні положення системи захисту інформації. Вимоги до захисту інформації Вимоги до системи захисту інформації. Види забезпечення системи захисту інформації. Особливості захисту даних фізичних осіб.*)* (РН6, РН13, РН16, РН19);

Теми лекційних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1.	Поняття інформаційної безпеки.	1	-
2.	Загрози інформаційної безпеки.	1	-
3.	Порушники інформаційної безпеки.	1	-
4.	Огляд законодавства в галузі інформаційної безпеки.	1	-
5.	Огляд міжнародних стандартів у галузі інформаційної безпеки.	1	-
6.	Адміністративний рівень інформаційної безпеки.	1	-
7.	Основні класи заходів організаційного рівня.	1	-
8.	Фізичні засоби захисту.	1	-
9.	Криптографічні засоби захисту.	2	-
10.	Особливості сучасних інформа ійних систем з погляду безпеки.	2	-
11.	Основні сервіси безпеки. Екранування.	2	-
12.	Система забезпечення інформаційної безпеки.	2	-
Разом		16	-

Теми практичних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1.	Практичне заняття №1. Поняття інформаційної безпеки.	1	-
2.	Практичне зайняття №2. Загрози інформаційної безпеки.	1	-
3.	Практичне заняття № 3. Порушники інформаційної безпеки.	1	-
4.	Практичне зайняття № 4. Законодавства в галузі інформаційної безпеки.	1	-
5.	Практичне заняття № 5. Міжнародні стандарти у галузі інформаційної безпеки.	1	-

6.	Практичне зайняття № 6. Адміністративний рівень інформаційної безпеки.	1	-
7.	Практичне зайняття № 7. Основні класи заходів організаційного рівня.	1	-
8.	Практичне зайняття №8. Фізичні засоби захисту.	1	-
9.	Практичне зайняття №9. Криптографічні засоби захисту.	1	-
10.	Практичне зайняття № 10. Особливості сучасних інформаційних систем з погляду безпеки.	1	-
11.	Практичне зайняття №11. Основні сервіси безпеки.	2	-
12.	Практичне зайняття № 12. Система забезпечення інформаційної безпеки.	2	-
	Разом	14	0

Форми та методи навчання

Методи навчання: демонстрація, навчальна дискусія; технології викладання: тренінги, аналіз конкретних ситуацій, обговорення, презентації, міні-лекції, ситуаційні дослідження, навчання на основі досвіду та інші.

Інструменти, обладнання, програмне забезпечення

Для опанування даного ОК необхідно мати постійний доступ до інтернету, інтернет сайтів, телефон або комп'ютер (ноутбук)

Порядок оцінювання програмних результатів навчання / результатів навчання

Для досягнення цілей та завдань курсу студентам потрібно вчасно виконати завдання пов'язане із пошуком інформації стосовно вибраної професійної діяльності, оформити у презентаційний вигляд та представити-захистити перед колективом студентів групи; вчасно здати модульні контролі знань.

Викладач проводить оцінювання індивідуальних завдань студентів шляхом проставлення балів за визначеними критеріями, що вчасно доводяться здобувачам освіти. Також, студент під наглядом викладача самостійно оцінює свою роботу.

За вчасне та якісне створення презентаційного завдання, студент отримує такі обов'язкові бали:

10 балів за вчасне (згідно визначеного графіка) виконання завдання;
- 10 балів за якісне оформлення завдання;
- 20 балів за представлення завдання;
- 20 балів за захист

та відповіді на запитання.

20 балів – модуль 1;
20 балів – модуль 2.

Усього 100 балів.

Студенти можуть отримати додаткові бали за: виконання рефератів, есе дослідницького характеру за темою курсу. Тему можуть дослідницької роботи вибрати самостійно за погодженням із викладачем. Додаткові бали студентам також можуть бути зараховані за конкретні пропозиції з удосконалення змісту навчальної дисципліни.

Модульний контроль проходитиме у формі тестування. У тесті 30 запитань різної складності: рівень 1 – 20 запитань по 0,4 бали (8 балів), рівень 2 – 8 запитань по 1 балу (8 балів), рівень 3 – 2 запитання по 2 бали (4 бали). Усього – 20 балів.

Вид заняття		**Бали**	**Форма контролю**
1. Поточна складова оцінювання			
1.	**Лекційні заняття**		
Змістовий модуль 1.			
1.1.1.	Тема №1. Поняття інформаційної безпеки	1	Комп'ютерне тестування шляхом складання модульного контролю
1.1.2.	Тема №2. Загрози інформаційної безпеки	1	
1.1.3.	Тема №3. Порушники інформаційної безпеки	1	
1.1.4.	Тема №4. Огляд законодавства в галузі інформаційної безпеки	1	
1.1.5.	Тема №5. Огляд міжнародних стандартів у галузі інформаційної безпеки	1	
1.1.6.	Тема №6. Адміністративний рівень інформаційної безпеки	1	
Змістовий модуль 2.			
1.1.7.	Тема №7. Основні класи заходів організаційного рівня	1	Комп'ютерне тестування шляхом складання модульного
1.1.8	Тема №8. Фізичні засоби захисту	1	
1.1.9	Тема №9. Криптографічні засоби захисту	2	
1.1.10	Тема № 10. Особливості сучасних інформаційних систем з погляду безпеки	2	
1.1.11	Тема №11. Основні сервіси безпеки. Екранування	2	
1.1.12	Тема № 12. Системи забезпечення інформаційної безпеки.	2	
Разом		16	
1.2. Практичні заняття			
1.2.1.	Практичне заняття № 1. Поняття інформаційної безпеки.	9	Виконання завдань.
1.2.2.	Практичне зайняття № 2. Загрози інформаційної безпеки.	9	
1.2.3.	Практичне заняття № 3. Порушники інформаційної безпеки.	9	

1.2.4.	Практичне зайняття № 4. Законодавство в галузі інформаційної безпеки.	9	
1.2.5.	Практичне заняття №5. Міжнародні стандарти у галузі інформаційної безпеки	8	
1.2.6.	Практичне зайняття № 6. Адміністративний рівень інформаційної безпеки.	8	
1.2.7.	Практичне зайняття № 7. Основні класи заходів організаційного рівня	8	
1.2.8.	Практичне зайняття №8. Фізичні засоби захисту.		
Усього бали за практичні заняття		60	
Усього бали за поточною складовою оцінювання:		**60**	
2. Модульна складова оцінювання			
2.1.	Модульний контроль №1	20	Комп'ютерне тестування
2.2.	Модульний контроль №2	20	Комп'ютерне тестування
Усього бали за підсумковою складовою оцінювання:		**40**	
Разом бали за освітню компоненту:		**100**	

Оцінювання завдань поточного (модульного) контролю*

Рівень складності завдань	**Кількість завдань в білеті**	**Оцінка завдань, балів**	
		за одне	**загальна**
1	20	0,4	8
2	9	1	9
3	1	3	3
Разом	30	X	20

* наводиться для усіх модульних контролів

Перелік нормативних документів університету що регулюють порядок оцінювання та проведення контрольних заходів:

- Положення про організацію освітнього процесу у Національному університеті водного господарства та природокористування (нова редакція) (Наказ №358 від 06.07.2020р) https://ep3.nuwm.edu.ua/4088/
- Порядок організації контролю та оцінювання навчальних досягнень студентів Національного університету водного господарства та природокористування (НУВГП) у Європейській кредитно-трансферній системі (ЄКТС) (зі змінами та доповненнями) (Наказ №168 від 04.04.2016р) https://ep3.nuwm.edu.ua/21121/;
- Положення про семестровий поточний та підсумковий контроль навчальних досягнень здобувачів вищої освіти (Наказ № 310 від 26.05.2019) – https://ep3.nuwm.edu.ua/15311/ – регламентує порядок проведення семестрового поточного (модульного) та підсумкового контролю навчальних досягнень здобувачів вищої освіти за освітніми ступенями бакалавра і магістра денної і заочної форми навчання в Національному університету водного господарства та природокористування, описує зміст і процедуру державної атестації, поточного, підсумкового та семестрового контролів;
- Система оцінювання результатів навчання здобувачів вищої освіти (семестровий поточний контроль) зі змінами та доповненнями (ухвалено науково-методичною радою НУВГП протокол №1 від 19.02.2020) https://ep3.nuwm.edu.ua/21123/ – описує критерії оцінювання навчальних досягнень та порядок рейтингування здобувачів вищої освіти;
- Методичні вказівки щодо формування, наповнення та оформлення сторінок навчальних дисциплін в Навчальній платформі НУВГП (для професорсько-викладацького складу) (схвалено науково-методичною радою НУВГП Протокол № 1 від 27.02.2019 р) http://ep3.nuwm.edu.ua/13934/ – описують порядок оформлення та створення тестів для семестрового поточного та підсумкового контролів, порядок завантаження науково-методичних джерел в курси;
- Інструкція для здобувачів вищої освіти щодо організації та проведення навчальних занять у дистанційній формі https://ep3.nuwm.edu.ua/19215/

Рекомендована література (основна, допоміжна)

Основна література

1. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, О. Д. Кожухівській, О. П. Войтович, – Черкаси: ЧДТУ, 2008. – 223 с.
2. Інформаційна безпека держави: навчальний посібник / В. М. Рудницький, С. О. Гнатюк, Н. В. Лада, Р. В. Бреус. - Харків : ТОВ «ДІСА ПЛЮС», 2018. – 359 с.
3. Лужецький В. А. Інформаційна безпека : навчальний посібник / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв – Вінниця : УНІВЕРСУМВінниця, 2009. – 240 с. – ISBN 978-966-641-265-5

Допоміжна література

4. Маланчук Л.О. Посилення стійкості інформаційного суверенітету України в сучасних умовах/ Зб.наук.пр.:Стратегія і тактика державного управління.- Рівне: НУВГП. 2016.Вип 3. С.28-36
5. Лужецький В. А. Захист персональних даних : навчальний посібник / В. А. Лужецький, О. П. Войтович, А. В. Дудатьєв – Вінниця : УНІВЕРСУМВінниця, 2009. – 240 с. – ISBN 978-966-641-317-1
6. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2009. – 608 с.
7. Закон України «Про інформацію» : за станом на 1 січня 2013 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12
8. Закон України «Про захист інформації в інформаційнотелекомунікаційних системах» : за станом на 1 січня 2013 р. / Верховна Рада України. — Офіц. вид. — Режим доступу до ресурсу: http://zakon.rada.gov.ua/cgibin/laws/main.cgi?nreg=80%2F94-%E2%F0
9. Нормативные акты Украины // www.nau.kiev.ua
10. Маланчук Л.О., Данилюк А.В. Аналіз системи інформаційної безпеки в Україні та пріорітети її удосконалення. Вісник Національного університету водного господарства та природокористування. Сер. Економічні науки. 2021. №4(96). С. 174-182. URL:http://visnyk.nuwm.edu.ua/index.php/econ/article/view/ve4202114/1024
11. Маланчук Л.О., Ковальова К.Ю. Роль та значення інформаційної безпеки в умовах воєнного стану //VIII Міжнародна науково-практична конференція «Modern research in word science», 29-31.10.2022 Львів, Україна. 2022. Ст. 935-938 https://sci-conf.com.ua/viii-mizhnarodna-naukovo-praktichna-konferentsiya-modern-research-in-world-science-29-31-10-2022-lviv-ukrayina-arhiv/.
12. Маланчук Л.О., Шульга К.А. Доступ до публічної інформації в умовах воєнного стану //VIII Міжнародна науково-практична конференція «Modern research in word science», 29-31.10.2022 Львів, Україна. 2022. Ст. 1611-1617 https://sci-conf.com.ua/viii-mizhnarodna-naukovo-praktichna-konferentsiya-modern-research-in-world-science-29-31-10-2022-lviv-ukrayina-arhiv/.

Інформаційні ресурси в Інтернет

1.https://www.google.com/search?

q=google&rlz=1C1GCEA_enUA988UA988&oq=Go&aqs=chrome.1.69i57j0i131i433i512l4j69i60l3.6544j0j7&sourceid=chrome&ie=UTF-8
2. Пошукова система у базі лекцій, наукових статей, навчальних посібників та підручників з усього світу/Google Академія - Режим доступу до ресурсу: http://scholar.google.com.ua/

Здобувачі можуть отримати доступ до таких міжнародних інформаційних ресурсів:
- електронні бібліотеки:
http://lib.nuwm.edu.ua/index.php/korisni-posilannya/elektronni-biblioteki
- Як знайти статтю у Scopus:
http://lib.nuwm.edu.ua/index.php/biblioteka/novini/item/506-v-dopomohu-avtoram
- База періодичних видань:
https://www.scimagoir.com/
- Можливості доступу до електронних ресурсів та сервісів: http://lib.nuwm.edu.ua/index.php/biblioteka/novini/item/516-mozhlyvosti-dostupu-do-resursiv-i-servisiv

Здобувачі можуть брати участь у Проєкті сприяння академічній доброчесності в Україні (SAIUP) https://nuwm.edu.ua/sp/akademichna-dobrochesnistj .

Поєднання навчання та досліджень*

Студенти мають можливість додатково отримати бали за виконання індивідуальних завдань дослідницького характеру, а також можуть бути долучені до написання та опублікування наукових статей з тематики курсу.

В освітньому процесі використовуються досягнення викладача курсу – керівника відділу якості освіти НУВГП – механізми та процедури в освітньому процесі університету https://nuwm.edu.ua/sp.

ПОЛІТИКИ ВИКЛАДАННЯ ТА НАВЧАННЯ

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

- творчі здібності;
- уміння працювати та взаємодіяти з людьми;
- клієнтоорієнтованість;
- гнучкість розуму;
- критичність мислення;
- працювати в команді;
- об'єктивне оцінювання особистих досягнень та ін.

Дедлайни та перескладання

Ліквідація академічної заборгованості здійснюється згідно «Порядку ліквідації академічних заборгованостей у НУВГП», http://ep3.nuwm.edu.ua/4273/. Згідно цього документу і реалізується право студента на повторне вивчення дисципліни чи повторне навчання на курсі. Перездача модульних контролів здійснюється згідно http://nuwm.edu.ua/strukturni-pidrozdili/navch-nauk-tsentr-nezalezhnoho-otsiniuvannia-znan/dokumenti. Оголошення стосовно дедлайнів здачі та перездачі оприлюднюються на сторінці MOODLE https://exam.nuwm.edu.ua/

Неформальна та інформальна освіта

Студенти мають право на перезарахування результатів навчання набутих у неформальній та інформальній освіті згідно відповідного Положення про неформальну освіту. http://ep3.nuwm.edu.ua/18660/.

На ресурсі - https://www.skeptic.in.ua/integrity/?fbclid=IwAR2TE9zaoPiVjFfH281AqWCB4Sl16GlCpmjfto6CvZ0eAN7efPpMM7LmuHY студенти зможуть знайти: офіційні документи і рекомендації, ФБ, Проєкт сприяння академічній доброчесності в Україні, вебінари, короткі відеопоради студентам, аналітика, книжки, монографії, системи виявлення текстових запозичень, кодекси етики, академічне письмо, дискусії, інфографіка.

Правила академічної доброчесності

Усі здобувачі виконані навчальні завдання самостійно перевіряють на виявлення текстових запозичень через університетську платформу MOODLE http://wiki.nuwm.edu.ua/index.php/Unplag.

В аудиторії здобувачі не допускаються до списування та обману – за порушення принципів академічної доброчесності викладач може накладати санкції: зниження балів, повернення роботи на доопрацювання, не допущення до захисту роботи та ін.

Вимоги до відвідування

Студенту не дозволяється пропускати заняття без поважних причин. Якщо є довідка про хворобу чи іншу поважну причину то студенту не потрібно відпрацьовувати пропущене заняття.

При об'єктивних причинах пропуску занять, студенти можуть самостійно вивчити пропущений матеріал на платформі MOODLE https://exam.nuwm.edu.ua/course/view.php?id=341

Здобувачі без обмежень можуть на заняттях використовувати мобільні телефони та ноутбуки.

Автор
Доцент Лариса МАЛАНЧУК

Затверджено {{JS:'[oSigner.sFIO_Referent]' ? '[OSIGNER.SFIO_REFERENT]':'[oSigner.sNameFamilyUpcase]'}}

документ підписаний КЕП
Номер документа СИЛ №358 від [sDateTime_SignWriteAgree_Last]
Підписувач СОРОКА ВАЛЕРІЙ СТЕПАНОВИЧ
Підписувач (дані КЕП): [oSignECP.sSigner_Sert]
Сертифікат 58E2D9E7F900307B04000000807E2D0054327D00