НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
Навчально-науковий інститут права

08-04-27S

СИЛАБУС		**SYLLABUS**
Інформаційна безпека		***Information Security***
Шифр за ОП	ВБ 6.1	Code in Degree Programme
Освітній рівень: магістерський (другий)		Educational level: master's (second)
Галузь знань **Журналістика**	06	Галузь знань **Журналістика**
Спеціальність **Журналістика**	061	Спеціальність **Журналістика**
Освітня програма: **Медіаправо та медіабезпека**		Degree Programme: **Media Law and Media Security**

РІВНЕ – 2025

Силабус навчальної дисципліни «***Інформаційна безпека***» для здобувачів вищої освіти ступеня «магістр», які навчаються за освітньо-професійною програмою програмою Медіаправо та медіабезпека, спеціальності 061 Журналістика Рівне. НУВГП. 2025. 16 стор.

ОП на сайті університету: http://ep3.nuwm.edu.ua/id/eprint/30396

Розробник силабусу: *Мітчук Ольга Андріївна, д. н. соц. ком., професор, професор кафедри інформаційного права та юридичної журналістики;*
Прокопець Віталій Едуардович, старший викладач кафедри інформаційного права та юридичної журналістики, начальник відділу зв'язків з громадськістю Національного університету водного господарства та природокористування, член Національної спілки журналістів України.

Силабус схвалений на засіданні кафедри *інформаційного права та юридичної журналістики*
Протокол № 12 від 03 липня 2025 року

в.о. завідувача кафедри: *Мітчук Ольга Андріївна, доктор наук із соціальних комунікацій, професор*

Керівник (гарант) ОП: *Мітчук Ольга Андріївна, доктор наук із соціальних комунікацій, професор кафедри інформаційного права та юридичної журналістики*

Схвалено науково-методичною радою з якості ННІП та ГН:
Протокол № 1 від 3 липня 2025 року
Голова науково-методичної ради з якості ННІП та ГН: *Цимбалюк Валерій Іванович, к.ю.н., професор.*

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «*Інформаційна безпека*»	
*Навчальна дисципліна «**Інформаційна безпека**» є освітнім компонентом вільного вибору за освітньою-професійною програмою «Медіаправо та медіабезпека» спеціальності 061 «Журналістика».*	
ЗАГАЛЬНА ІНФОРМАЦІЯ	
Ступінь вищої освіти	*магістр*
Освітня програма	*«Медіаправо та медіабезпека»*
Спеціальність	*061 – Журналістика*
Рік навчання, семестр	*Рік навчання – 2, семестр – 3*
Кількість кредитів	*3*
Лекції:	*Для денної форми навчання – 10* *Для заочної форми навчання - 4*
Практичні заняття:	*Для денної форми навчання – 20* *Для заочної форми навчання - 6*
Лабораторні заняття:	*-*
Самостійна робота:	*Для денної форми навчання – 60* *Для заочної форми навчання - 80*
Всього	*90*
Курсова робота:	*-*
Форма навчання	*Денна, заочна*
Форма підсумкового контролю	*залік*
Мова викладання	*державна*
ІНФОРМАЦІЯ ПРО РОЗРОБНИКА	
Лектор 	*Мітчук Ольга Андріївна, д.н. із соц.ком., професор кафедри конституційного права та галузевих дисциплін*
Вікіситет	Wikiситет Ольга Мітчук
ORCID	*https://orcid.org/0000-0002-1011-7320*
Як комунікувати	o.a.mitchuk@nuwm.edu.ua

	*Прокопець Віталій Едуардович, старший викладач кафедри інформаційного права та юридичної журналістики, начальник відділу зв'язків з громадськістю, член Національної спілки журналістів України*
Вікіситет	*Віталій Прокопець*
ORCID	
Як комунікувати	*v.e.prokopets@nuwm.edu.ua*

ІНФОРМАЦІЯ ПРО ОСВІТНІЙ КОМПОНЕНТ

Мета та завдання

Метою викладання дисципліни «Інформаційна безпека» є формування у здобувачів вищої освіти комплексних знань, умінь та практичних навичок, необхідних для розуміння загроз інформаційній безпеці, принципів її забезпечення, а також застосування сучасних методів та засобів захисту інформації в різних сферах діяльності. Дисципліна має на меті підготувати фахівців, здатних ідентифікувати, аналізувати та ефективно протидіяти кіберзагрозам, забезпечуючи конфіденційність, цілісність та доступність інформації.

***Завданнями навчальної дисципліни є**:*

- **Ознайомлення з основними поняттями та принципами інформаційної безпеки**: вивчення визначень, складових інформаційної безпеки (конфіденційність, цілісність, доступність), класифікації загроз та вразливостей.
- **Вивчення нормативно-правового забезпечення інформаційної безпеки**: надання знань щодо національних та міжнародних законодавчих актів, стандартів та регуляторних вимог у сфері кібербезпеки та захисту інформації.
- **Аналіз методів та засобів захисту інформації**: розгляд програмних, апаратних, організаційних та фізичних методів захисту інформації, криптографічних засобів, систем виявлення вторгнень.
- **Навчання управління ризиками інформаційної безпеки**: формування навичок з ідентифікації, оцінки та мінімізації ризиків, розробки політик безпеки.
- **Освоєння основ аудиту та моніторингу інформаційної безпеки**: вивчення методів проведення аудиту безпеки, моніторингу подій та реагування на інциденти.
- **Розвиток практичних навичок з використання засобів захисту**: робота з антивірусним програмним забезпеченням, фаєрволами, системами резервного копіювання тощо.
- **Набуття знань про особливості захисту інформації** в різних інформаційних системах (корпоративні мережі, веб-ресурси, хмарні технології, мобільні пристрої).
- **Розгляд питань кіберзлочинності та кібервійни**: ознайомлення з основними видами кіберзлочинів, методами їх розслідування та протидії.

Посилання на розміщення освітнього компонента на навчальній платформі Moodle

Передумови вивчення* (місце освітнього компоненту в структурно-логічній схемі)

*При вивченні освітньої компоненти «**Інформаційна безпека**» використовуються та розширюються компетентності, які набуваються здобувачами при вивченні дисциплін «Медіабезпека та інформаційне суспільство», «Медіаправо та журналістика розслідувань».*

Компетентності

ІК – Здатність розв’язувати задачі дослідницького та/або інноваційного характеру у сфері журналістики.
ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК05. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК08. Здатність спілкуватися з представниками інших професійних груп різного рівня.
СК01. Здатність використовувати спеціалізовані концептуальні знання з теорії та історії журналістики, новітні технологічні досягнення для розв’язання задач дослідницького та/ або інноваційного характеру у сфері журналістики / медіаправа.
СК02. Здатність критично осмислювати проблеми у сфері журналістики та дотичні до них міждисциплінарні проблеми.
СК05. Здатність зрозуміло і недвозначно доносити власні висновки з питань журналістики, а також знання та пояснення, що їх обґрунтовують, до фахівців і нефахівців, зокрема до осіб, які навчаються.
СК06. Здатність інтегрувати знання та розв’язувати складні задачі журналістики у широких та/або мультидисциплінарних контекстах, за умов неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.

Програмні результати навчання (ПРН). Результати навчання (РН)*

РН01. Приймати ефективні рішення з проблем журналістики, у тому числі в умовах багатокритерійності, неповних чи суперечливих інформації та вимог.
РН05. Генерувати нові ідеї та використовувати сучасні технології під час створення медіапродуктів.
РН08. Використовувати передові знання і методики у процесі дослідження діяльності та створення нових медіаінституцій.
РН10. Мати практичні навички розв’язання проблем, пов’язаних з організацією нових медіаустанов та інституцій.
РН11. Брати продуктивну участь у розробленні проєктів документів, що регламентують діяльність в усіх сферах журналістики, обґрунтовувати суспільну потребу в їх прийнятті, прогнозувати результати їх впливу на суспільство.
РН14. Приймати рішення та розв’язувати професійні завдання з позицій соціальної відповідальності, верховенства права та дотримання законодавства

Структура та зміст освітнього компонента

Тема	РН	Форми організації навчання	Кількість годин	
			денна форма навчання	заочна форма навчання
Тема 1: Основи та принципи інформаційної безпеки 1. Поняття інформаційної безпеки: конфіденційність, цілісність, доступність. 2. Класифікація загроз інформаційній безпеці: випадкові, навмисні, зовнішні, внутрішні. 3. Основні принципи побудови системи захисту інформації.	01, 05	Л	2	1
		ПР	4	1
		СР	12	16
Тема 2: Нормативно-правове	08, 11	Л	2	

Законодавство України у сфері інформаційної та кібербезпеки: ключові закони та нормативні акти. 2. Міжнародні стандарти та рекомендації з інформаційної безпеки (ISO 27001, NIST). 3. Правові аспекти захисту персональних даних (GDPR) та критичної інфраструктури.		ПР	4	1
Тема 3: Методи та засоби захисту інформації 1. Криптографічні методи захисту інформації: шифрування, електронний підпис, хешування. 2. Організаційні та технічні засоби захисту: розмежування доступу, автентифікація, фаєрволи, системи виявлення вторгнень. 3. Програмне та апаратне забезпечення для захисту інформації: антивіруси, системи резервного копіювання, VPN.	08, 11, 14	Л	2	1
		ПР	4	1
		СР	12	16
Разом модуль 1		**Л**	**6**	**2**
		ПР	**12**	**3**
		СР	**36**	**48**
Тема 4: Управління ризиками та інцидентами інформаційної безпеки 1. Методології оцінки ризиків інформаційної	11, 14	Л	2	1
		ПР	4	1

політик інформаційної безпеки та планів реагування на інциденти. 3. Аудит та моніторинг інформаційної безпеки: цілі, методи та інструменти.				
		СР	12	16
Тема 5: Захист інформації в різних інформаційних системах та кіберзлочинність 1. Особливості захисту інформації в комп'ютерних мережах та хмарних сервісах. 2. Безпека веб-ресурсів та мобільних додатків. 3. Кіберзлочинність: види, методи протидії та розслідування кіберзлочинів.	05, 08, 10	Л	2	1
		ПР	4	2
		СР	12	16
Разом модуль 2		**Л**	**4**	**2**
		ПР	**8**	**3**
		СР	**24**	**32**
ВСЬОГО		**Л**	**10**	**4**
		ПР	**20**	**6**
		СР	**60**	**80**

Форми та методи навчання

Форми проведення занять*: традиційні лекції та практичні заняття, дуальні заняття із залученням практиків.*
Форми організації освітнього процесу: *навчальні заняття, самостійна робота, індивідуальні завдання, контрольні заходи.*
Особливості практичної підготовки: *вирішення ситуаційних завдань, наукові дослідження; дискусії; долучення до занять фахівців-практиків.*
Технології викладання: *рольові ігри, аналіз конкретних ситуацій, обговорення, презентації, міні-лекції, ситуаційні дослідження, навчання на основі досвіду та інші.*
Види навчальної роботи студента: практичні завдання, *навчальна дискусія, дебати опитування, ситуативні вправи, ділова гра, індивідуальне науково-дослідне завдання.*

Інструменти, обладнання, програмне забезпечення

Мультимедійна-, проекційна апаратура (проектори, екрани, смартдошки тощо), комп'ютери, інтернет мережі, бібліотечні фонди, законодавча база України у відкритому доступі. В якості навчальної платформи застосовується відкрита (Open Source) система управління навчанням Moodle.

Порядок оцінювання програмних результатів навчання/результатів навчання

Вид занять	Бали	Форма контролю
Поточна складова		

Основи та принципи інформаційної безпеки Мета: Поглибити розуміння студентами базових концепцій інформаційної безпеки та їхньої важливості для сучасного суспільства. Завдання: 1. Обґрунтуйте, чому поняття конфіденційності, цілісності та доступності інформації є взаємопов'язаними і однаково важливими для забезпечення комплексної безпеки. 2. Визначте щонайменше п'ять видів загроз інформаційній безпеці, з якими може зіткнутися типова організація, та наведіть приклади для кожної. 3. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте відомий випадок порушення інформаційної безпеки (наприклад, витік даних великої компанії, атака вірусу-здирника). Запропонуйте першочергові кроки, які мала б зробити організація для мінімізації шкоди та відновлення довіри.		***Методи та технології навчання*** – демонстрація та обговорення ***Форма контролю*** – практичне заняття з виступами студентів

Практичне заняття 2: Нормативно-	**10**	***Форми проведення занять*** – *практичне заняття*

Мета: Ознайомити студентів з основними нормативно-правовими актами у сфері інформаційної безпеки та їх застосуванням. Завдання: 1. Обґрунтуйте необхідність гармонізації українського законодавства у сфері захисту персональних даних з міжнародними стандартами, такими як GDPR. 2. Визначте ключові вимоги Закону України «Про основні засади забезпечення кібербезпеки України» до суб'єктів критичної інфраструктури. 3. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте випадок, коли організація зазнала санкцій за недотримання вимог щодо захисту персональних даних (наприклад, згідно з GDPR). 4. Запропонуйте план заходів, які організація мала б вжити, щоб відповідати цим вимогам.		***Методи та технології навчання*** – демонстрація та обговорення ***Форма контролю*** – практичне заняття з виступами студентів
Практичне заняття 3: Методи та засоби захисту	**10**	***Форми проведення занять*** – *практичне заняття* ***Методи та технології***

застосовувати різні методи і засоби захисту інформації. Завдання: 1. Обґрунтуйте, чому використання лише програмних засобів захисту (наприклад, антивірусу) недостатньо для забезпечення комплексної інформаційної безпеки. 2. Визначте основні переваги та недоліки симетричного та асиметричного шифрування та наведіть приклади їх застосування. 3. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте сценарій кібератаки на корпоративну мережу (наприклад, фішинг, DDoS-атака). 4. Запропонуйте комбінацію організаційних та технічних засобів захисту, яка могла б запобігти або мінімізувати наслідки такої атаки.		
Практичне заняття 4: Управління ризиками та інцидентами інформаційної безпеки Мета: Розвинути у студентів навички	**10**	***Форми проведення занять*** *– практичне заняття* ***Методи та технології навчання*** *– демонстрація* ***Форма контролю*** *– групове опитування студентів*

та реагування на інциденти. Завдання: 1. Обґрунтуйте важливість проактивного управління ризиками інформаційної безпеки порівняно з реагуванням на вже існуючі загрози. 2. Визначте ключові етапи плану реагування на інцидент інформаційної безпеки (наприклад, виявлення, локалізація, усунення, відновлення). 3. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте гіпотетичний інцидент, пов'язаний з витоком конфіденційної інформації з компанії. 4. Запропонуйте дії для команди безпеки відповідно до етапів реагування на інцидент.		
Практичне заняття 5: Захист інформації в	**10**	***Форми проведення занять*** – *практичне заняття*

Мета: Ознайомити студентів з особливостями захисту інформації в різних інформаційних системах та основними аспектами кіберзлочинності. Завдання: 1. Обґрунтуйте, чому безпека мобільних додатків вимагає особливого підходу порівняно з безпекою традиційних веб-ресурсів. 2. Визначте основні види загроз для хмарних сервісів та запропонуйте методи їх мінімізації. 3. Розгляньте аналіз конкретних ситуацій (Case-study): Проаналізуйте реальний випадок кіберзлочину (наприклад, фінансове шахрайство через інтернет, злам акаунтів). 4. Запропонуйте превентивні заходи для користувачів та організацій, а також перші кроки у випадку виявлення подібного злочину.		***Методи та технології навчання*** *– демонстрація презентації та аналіз конкретних ситуацій* ***Форма контролю*** *– обговорення кейсів*
Усього практичні заняття	**50**	
Індивідуальне науково-дослідне завдання	**10**	Наукова стаття, або тези або реферат.

2.1 Модульний контроль №1	20	Тести
2.2 Модульний контроль №2	20	Тести
Усього підсумкова складова оцінювання:	40	
РАЗОМ	**100**	

Основна література:

1. Збірник документів Ради Європи. Безпека журналістів // [Електронний ресурс]. – Режим доступу: https://rm.coe.int/16806b5970, вільний. – Назв. з екрану (дата звернення: 25.08.2023). 47
2. Кодекс практики Європейського Союзу щодо протидії дезінформації // [Електронний ресурс]. – Режим доступу: https://www.nrada.gov.ua/foreign_practice/, вільний. – Назв. з екрану (дата звернення: 25.08.2023).
3. Посібник до навчального курсу щодо безпеки журналістів. Курс розроблено спільно трьома інституціями: Національною школою суддів, Національною академією внутрішніх справ і Тренінговим центром прокурорів України за підтримки Проєкту «Європейський Союз та Рада Європи працюють разом для підтримки свободи медіа в Україні». // // [Електронний ресурс]. – Режим доступу: https://rm.coe.int/bezpekazhurnalistiv-posibnyk-final-print-1-/1680a3f8df, вільний. – Назв. з екрану (дата звернення: 25.08.2023).
4. Посібник з верифікації. Визначний гід з верифікації цифрового контенту для висвітлення надзвичайних подій // [Електронний ресурс]. – Режим доступу: https://verificationhandbook.com/book_ua/chapter8.php#, , вільний. – Назв. з екрану (дата звернення: 25.08.2023).
5. Посібник з безпеки для журналістів: Посібник для репортерів у небезпечних зонах. Reporters sans frontières (France), 2022 //[Електронний ресурс]. – Режим доступу: https://unesdoc.unesco.org/ark:/48223/pf0000381168, вільний. – Назв. з екрану (дата звернення: 25.08.2023).
6. Україна Висвітлення конфлікту в Україні: практичний посібник для журналістів // // [Електронний ресурс]. – Режим доступу: https://www.thomsonfoundation.org/media/33402/ukraine1203bleed_ukr_preview.pdf, вільний. – Назв. з екрану (дата звернення: 25.08.2023).
7. Цифрова безпека журналіста-розслідувача // [Електронний ресурс]. – Режим доступу: https://video.detector.media/lessons/cyfrova-bezpekazhurnalista-rozsliduvacha-i19, вільний. – Назв. з екрану (дата звернення: 25.08.2023).
8. Sydorenko, N., Mitchuk, O., Holik, O., Havryliuk, I., Myronets, N. Improving the Financial Stability of IT Companies through Social Media Marketing. WSEAS Transactions on Business and Economics 2022, 19, pp. 1621–1632 (Scopus).
9. Bessarab, A., Mitchuk, O., Baranetska, A.,. Kvasnytsia, O., Mykytiv, G. Social networks as a phenomenon of the information society. Journal of Optimization in Industrial Engineering, 2021, 14(1), pp. 35–42 (Scopus).

Додаткова література:

10. Безпека інформації: навч. посіб. / Інститут масової інформації // [Електронний ресурс]. – Режим доступу: http://imi.org.ua/bezpeka/spravochnik-po-bezopasnosti
11. Безпека журналістів в Україні: існуючі виклики і шляхи їх подолання // [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubricpresshall/3099965-bezpeka-zurnalistiv-v-ukraini-isnuuci-vikliki-ta-slahi-ihpodolanna.html
12. Вальорска М. Аґнєшка. Діпфейк та дезінформація: практ. посіб. / Аґнєшка М. Вальорска; пер. з нім. В. Олійника – К.: Академія української преси; Центр Вільної Преси, 2020. – 36 с. // [Електронний ресурс]. – Режим доступу: https://www.aup.com.ua/uploads/DEEPFAKES_FNF_AUP_2020.pdf
13. Верховна Рада посилила відповідальності за злочини 48ротии журналістів // [Електронний ресурс]. – Режим доступу: https://detector.media/community/article/184510/2021-02-02-verkhovna-radaposylyla-vidpovidalnosti-za-zlochyny-proty-zhurnalistiv/
14. Вступ до безпеки. Онлайн-курс з громадянської журналістики // [Електронний ресурс]. – Режим доступу: https://school-cj.org/courses/security
15. Гарантії забезпечення свободи слова (інформація підготовлена з використанням

16. «Гендер в деталях» випустив серію жартівливих картинок для журналістів на тему сексизму // [Електронний ресурс]. – Режим доступу: http://imi.org.ua/news/hender-v-detalyah-vypustyv-seriyu-zhartivlyvyh-kartynokdlyal-zhurnalistiv-na-temu-seksyzmu/
17. Довідник безпеки журналістів // [Електронний ресурс]. – Режим доступу: http://www.cje.org.ua/sites/default/files/library/Dovydnik-bezpekigurnalistiv.pdf
18. Земляна І., Романюк О. Журналіст і (НЕ) безпека. Посібник для журналістів, які працюють в небезпечних умовах / І. Земляна, О. Романюк [Текст] // [Електронний ресурс]. – Режим доступу: http://imi.org.ua/wpcontent/uploads/2017/06/Zhurnalist-i-nebezpeka.pdf
19. Зубченко Я. Я. Погляд у майбутнє. Чого досягли окуляри доповненої реальності / Я. Зубченко [Текст] // [Електронний ресурс]. – Режим доступу: https://ms.detector.media/trendi/post/26194/2020-12-15-poglyad-u-maybutniechogo-dosyagly-okulyary-dopovnenoi-realnosti/
20. Інститут масової інформації створив сайт з безпеки для журналістів // [Електронний ресурс]. – Режим доступу: http://detector.media/infospace/article/118301/2016-08-31-institut-masovoiinformatsii-stvoriv-sait-z-bezpeki-dlya-zhurnalistiv/
21. Інформаційна безпека: соціально-правові аспекти: Підручник. Остроухой Б. В., Петрик Б. М., Прнсяжнюк М. М. та ін.; за заг. ред. Є. Д. Скулиша. – К. КНТ, – 776 с. // [Електронний ресурс]. – Режим доступу: http://www.dut.edu.ua/uploads/l_1352_84114000.pdf
22. Кастельс М. Інтернет-Галактика.– К.: Ваклер. 2007. – 290 с. 28. Категорія: цифрова безпека // [Електронний ресурс]. – Режим доступу: http://j-sos.org.ua/category/novyny/tsyfrova-bezpeka/

Інформаційні ресурси в Інтернет

Цифрова безпека журналістів та інших працівників медіа. Prometheus // https://courses.prometheus.org.ua/courses/coursev1:Prometheus+DSJ101+2022_T1/about
Сайт Arcуспільного мовлення https://suspilne.media/ 20. Умови та правила Facebook https://ru-ru.facebook.com/policies
Сайт Організації Об'єднаних націй https://www.un.org/ru/
Сайт Європейського суду з прав людини - https://www.echr.coe.int/Pages/home.aspx?p=applicants/ukr&c
Сайт справ Європейського суду з прав людини - https://hudoc.echr.coe.int/rus
Сайт Міністерства інформаційної політики України https://mip.gov.ua/
Сайт Центру демократії та верховенства права https://cedem.org.ua/
Сайт Харківської правозахисної групи http://khpg.org/
Сайт Незалежної медійної ради: www.mediarada.org

Поєднання навчання та досліджень* *(за потреби)*

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.

ПОЛІТИКИ ВИКЛАДАННЯ ТА НАВЧАННЯ

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

Перелік соціальних, «м'яких» навичок (soft skills), які здобувач освіти здобуває під час вивчення ОК «***Інформаційна безпека***» формуються такі soft skills: *Здатність логічно обґрунтовувати свою позицію, здатність до навчання, знаходити вихід із складних ситуацій, ініціативність, вміння працювати в команді, комплексне рішення проблем, формування власної думки, уміння слухати та запитувати та інші.*

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://ep3.nuwm.edu.ua/15311/ . Оголошення стосовно дедлайнів здачі та перездачі оприлюднюються на сторінці MOODLE https://exam.nuwm.edu.ua/

Неформальна та інформальна освіта (за потреби)

Студенти мають право на перезарахування результатів навчання

важливо, щоб знання та навички, що формуються під час проходження певного онлайн-курсу чи його частин, мали зв'язок з очікуваними навчальними результатами даної дисципліни/ освітньої програми та перевірялись в підсумковому оцінюванні.

Правила академічної доброчесності
Здобувачі вищої освіти повинні дотримуватися «Кодексу честі студентів» https://ep3.nuwm.edu.ua/4917/ . Перевірку навчальних завдань неупереджено здійснює викладач. Усі навчальні завдання повинні бути виконанні власноручно здобувачем вищої освіти, у разі виявлення однакових робіт, здобувач освіти не отримує бали і повинен виконати завдання повторно. 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
Відпрацювати пропущені заняття студенти можуть шляхом самостійного вивчення лекційного матеріалу та виконання практичних завдань із відповідних тем. При цьому пропущене усне опитування можна відпрацювати на консультації. Використання мобільних телефонів, планшетів та ноутбуків для вирішення практичних завдань на заняттях дозволяється, окрім контрольних заходів (опитування, тестування тощо).

Автор Ольга МІТЧУК

Автор
В.о. завідувача кафедри ІПЮЖ Ольга МІТЧУК

Затверджено

Проректор з науково-педагогічної та навчальної роботи Валерій СОРОКА

документ підписаний КЕП
Номер документа СИЛ №959
Підписувач Сорока Валерій Степанович
Підписувач (дані КЕП):
Сертифікат 3FAA9288358EC003040000009B6C3700C8C2C100