НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

"ЗАТВЕРДЖУЮ"
Декан
гуманітарно-педагогічного факультету
Інна САВИЦЬКА
"27" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем,
мереж та кібербезпеки
Протокол №10 від «17» травня» 2023р.
завідувач кафедри
Дмитро КАСАТКІН

РОЗГЛЯНУТО
Гарант ОП «Журналістика»
_____ Марина НАВАЛЬНА

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Цифрова безпека медіа»

Спеціальність	061 «Журналістика»
Освітня програма	06 «Журналістика»
Факультет	інформаційних технологій
Розробник:	докт.техн.наук, проф. Лахно В.А.

Київ – 2023 рік

1. Опис навчальної дисципліни
Цифрова безпека медіа

(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	061 «Журналістика»	
другий (магістерський) рівень	Магістр	
Характеристика навчальної дисципліни		
Вид	Обов'язкова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2023-2024	
Семестр	1	
Лекційні заняття	30 год.	
Практичні, семінарські заняття	30 год.	
Лабораторні заняття	-	
Самостійна робота	90 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних		

1. Мета та завдання навчальної дисципліни

Мета - Курс покликаний навчити журналістів та інших працівників медіа основ цифрового захисту для активного використання набутих навичок у професійному житті.

Завдання навчальної дисципліни «Цифрова безпека медіа» - є теоретична та практична підготовка магістрантів до розробки та застосування сучасних програмно-апаратних систем кібербезпеки в різних установах.

Інтегральна компетентність - Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі журналістики та галузях, що забезпечують інформаційний супровід, прогнозувати динаміку суспільного розвитку та задовольняти інформаційні потреби, що передбачає застосування положень і методів соціально-комунікаційних та інших наук, проведення досліджень та характеризується невизначеністю умов.

Навчальна дисципліна забезпечує формування ряду загальних та фахових компетентностей:

ЗК06. Здатність приймати обґрунтовані рішення.

ЗК09. Здатність оцінювати та забезпечувати якість виконуваних робіт.

СК01. Здатність використовувати спеціалізовані концептуальні знання з теорії та історії журналістики, новітні технологічні досягнення для розв'язання задач дослідницького та інноваційного характеру у сфері журналістики.

СК03. Здатність приймати ефективні рішення у сфері журналістики.

СК09. Здатність створювати контент для інформаційного супроводу агросектору та ефективно просувати медійний продукт.

У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме

ПРН02. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан та розвиток журналістики.

ПРН03. Проводити збір, інтегрований аналіз матеріалів з різних джерел, включаючи наукову та професійну літературу, бази даних, та перевіряти їх на достовірність, використовуючи сучасні методи досліджень.

ПРН08. Використовувати передові знання і методики у процесі дослідження діяльності та створення нових медіаінституцій.

ПРН12. Розробляти та реалізовувати інноваційні та дослідницькі проєкти у сфері журналістики з урахуванням правових, соціальних, економічних та етичних аспектів

ПРН15. Створювати якісний контент для інформаційного супроводу агросектору.

3. Програма та структура навчальної дисципліни для:

– повного терміну денної (заочної) форми навчання

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Політика інформаційної безпеки медіа інституції.												
Тема 1. Властивості інформації з точки зору проблематики її захисту.	8	2	-			6						
Тема 2. Ризики порушення політики інформаційної безпеки медіа інституції. Вимоги щодо безпеки системи, ризики безпеки.	13	3	4			6						
Тема 3. Механізми реалізації послуг безпеки.	14	4	4			6						
Тема 4. Поняття загрози інформації.	12	2	4			6						
Тема 5. Політика інформаційної безпеки (ІБ).	10	2	2			6						
Тема 6. Аналіз безпеки програмного забезпечення.	15	3	2			10						
Разом за змістовим модулем 1	**72**	**16**	**16**			**40**						
Змістовий модуль 2. Аналіз безпеки об'єктів медіа інституції.												
Тема 7. Загрози цифровій безпеці медіа інституції. Найпоширеніші інциденти безпеки, що трапляються з журналістами.	23	4	4			15						
Тема 8. Методи захисту інформації.	23	4	4			15						
Тема 9. Задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в комп'ютерних системах.	14	2	2			10						
Тема 10. Криптографічний захист інформації.	18	4	4			10						

Разом за змістовим модулем 2	**78**	**14**	**14**			**50**						
Усього годин за курс	**150**	**30**	**30**			**90**						

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз ризиків порушення політики інформаційної безпеки об’єкта інформатизації (ОБІ), зокрема медіа інституції.	2
2	Аналіз вимог щодо безпеки ОБІ, зокрема медіа інституції.	2
3	Планування заході що до впровадження механізмів реалізації послуг безпеки.	4
4	Аналіз моделей безпеки інформаційно-комунікаційних систем (ІКС).	4
5	Аналіз безпеки програмного забезпечення для ОБІ.	2
6	Планування методів захисту інформації в ІКС.	4
7	Автентифікація користувачів у ІКС ОБІ.	4
8	Застосування криптографічного захисту інформації у ІКС ОБІ.	4
9	Способи відновлення доступу та як ними можуть скористатися зловмисники.	4
	Разом за семестр	**30**
	Разом	**30**

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Властивості інформації з точки зору проблематики її захисту та кібербезпеки об’єкту інформатизації (ОБІ) , зокрема медіа інституції.	8
2	Ризики порушення політики інформаційної безпеки ОБІ, зокрема медіа інституції.	8
3	Сучасні вимоги щодо безпеки системи, ризики безпеки ОБІ, зокрема медіа інституції.	8
4	Механізми реалізації послуг безпеки ОБІ, зокрема медіа інституції.	8
5	Політика інформаційної безпеки ІКС або ОБІ. Поняття загрози інформації.	8
6	Моделі безпеки ІКС.	8
7	Проблематика безпеки програмного забезпечення.	8
8	Інноваційні методи захисту інформації в ІКС.	8
9	Автентифікація користувачів на ОБІ та у ІКС підприємств.	9
10	Криптографічний захист інформації.	9
11	Криптографічні протоколи.	8
	Разом	**90**

6. Зразки контрольних питань, тестів для визначення рівня засвоєння знань студентами

1. Криза забезпечення безпеки інформації в сучасних інформаційно- телекомунікаційних системах (ІТКС).
2. Проблеми теорії захисту інформації.

3. Властивості інформації з точки зору ЗІ.
4. Використання поняття ризику.
5. Механізми реалізації послуг безпеки.
6. Механізми і політики розмежування прав доступу в ІКС.
7. Засоби забезпечення захисту інформації в ІКС.
8. Засоби ідентифікації й автентифікації об'єктів баз даних, управління доступом.
9. Засобу контролю цілісності інформації, організація аудиту.
10. Види загроз для інформаційної безпеки (ІБ).
11. Дестабілізуючі факторі.
12. Модель загроз для середовищ опрацювання інформації.
13. Дискреційна політика безпеки.
14. Мандатна політика безпеки.
15. Рольова політика безпеки.
16. Модель виявлення порушень.
17. Нелегітимне використання ресурсів.
18. Нелегітимний доступ до даних.
19. Нелегітимний запуск програм.
20. Нелегітимне виконання програм.
21. Нелегітимна відмова в обслуговування (порушення доступності).
22. Канали витоку інформації в ІКС та мережах.
23. Категорії уразливостей ІТКС.
24. Класи атак.
25. Шифрування даних.
26. Протоколи автентифікації.

7. Методи навчання

Проведення лекцій з використанням технічних засобів навчання. Проведення практичних робіт та самостійної роботи засобами інформаційно-комунікаційних технологій в освіті. Використовується електронний навчальний курс на платформі Moodle «Цифрова безпека медіа».

8. Форми контролю

Наприкінці кожного змістовного модуля проводиться контрольна робота у вигляді тесту, що створений у комп'ютерному навчальному середовищі. Підсумкова атестація: іспит.

9. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

Оцінка виконання та захисту практичних робіт за кожний модуль здійснюється у наступній відповідності:

№ Практичної роботи	**Кількість балів**	**Загальна кількість балів**

1 модуль		
Практична робота № 1	10	70
Практична робота № 2	10	
Практична робота № 3	10	
Практична робота № 4	10	
Практична робота № 5	10	
Самостійна робота	20	
Модульна контрольна		30
2 модуль		
Практична робота № 6	10	70
Практична робота № 7	10	
Практична робота № 8	10	
Практична робота № 9	20	
Самостійна робота	20	
Модульна контрольна		30

10. Навчально-методичне забезпечення

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання практичних робіт, глосарій термінів тощо.

11. Рекомендовані джерела інформації

Базові

1. 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.

2. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.).

3. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.

4. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.

Допоміжні

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S., ... & Florov, S. (2021). Synergy of building cybersecurity systems.