# СИЛАБУС ДИСЦИПЛІНИ
## «Цифрова безпека медіа»

**Ступінь вищої освіти – Магістр**
**Спеціальність 061 «Журналістика»**
**Освітня програма «Журналістика»**
**Рік навчання 1, семестр 2**
**Форма навчання** денна
**Кількість кредитів ЄКТС 5**
**Мова викладання** українська

| | |
|---|---|
| **Лектор курсу** |  **Лахно Валерій Анатолійович, д.т.н., професор (портфоліо)** |
| **Контактна інформація лектора (e-mail)** | **Кафедра комп'ютерних систем, мереж та кібербезпеки корпус. 15, к. 207, тел. 0445278724 e-mail lva964@nubip.edu.ua** |
| **Сторінка курсу в eLearn** | **ЕНК (2 семестр)** https://elearn.nubip.edu.ua/course/view.php?id=4571 |

## ОПИС ДИСЦИПЛІНИ

Курс покликаний навчити журналістів та інших працівників медіа основ цифрового захисту для активного використання набутих навичок у професійному житті. Вивчаються методологічні, організаційні та наукові основи розробки апаратно-програмних засобів і систем збору та захисту інформації (ЗІ), забезпечення інформаційної безпеки процесів опрацювання, зберігання та поширення інформації в інформаційно-комунікаційних мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем і засобів здійснення погроз з боку потенційних порушників.

**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.

**Зробимо курс корисним для вас. Якщо ви будете наполегливо працювати і докладати особливих зусиль, щоб не відставати від теоретичного та практичного матеріалу, ви отримаєте винагороду – як в короткостроковій перспективі, так і в набутті фахових компетентностей. Будь-ласка, широко використовуйте аудиторні заняття, відеоінструкції на ЕНК, вебінари, щоб переконатися, що рухаєтесь за графіком навчання**.

## СТРУКТУРА КУРСУ

| Тема | Години (лекції/ Лаб.) | Результати навчання | Завдання | Оцінювання |
|---|---|---|---|---|
| **2 семестр** | | | | |
| **Модуль 1. Політика інформаційної безпеки медіа інституції.** | | | | |
| Тема 1. Властивості інформації з точки зору проблематики її захисту. | **2/0** | Вміти здійснювати формалізований опис політик інформаційної безпеки для об'єктів захисту, зокрема для медіа. | Опитування. | **10** |
| Тема 2. Ризики порушення політики інформаційної безпеки. Вимоги щодо безпеки системи, ризики безпеки. | **3/4** | Вміти здійснювати формалізований опис політик інформаційної безпеки для об'єктів захисту, зокрема для медіа. | Захист практичної роботи. | **10** |
| Тема 3. Механізми реалізації послуг безпеки. | **4/4** | Вміти аналізувати ПЗ з точки зору безпеки його використовування в ІКС, зокрема для медіа. Вміти розробляти моделі загроз та порушника. Вміти здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання засобів захисту в умовах реалізації загроз різних класів. | Захист практичної роботи. | **10** |
| Тема 4. Поняття загрози інформації. | **2/4** | | Захист практичної роботи. | **10** |
| Тема 5. Політика інформаційної безпеки (ІБ). | **2/2** | | Захист практичної роботи. | **10** |
| Тема 6. Аналіз безпеки програмного забезпечення. | **3/2** | | Захист практичної роботи. | **10** |
| **Самостійна робота** | | | | **10** |
| **Модульний контроль** | | | Підсумковий тест в ЕНК | **30** |
| **Модуль 2. Аналіз безпеки об'єктів медіа інституції.** | | | | |
| Тема 7. Загрози цифровій безпеці медіа інституції. Найпоширеніші інциденти безпеки, що трапляються з журналістами. | **4/4** | Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки | Захист практичної роботи. | **10** |
| Тема 8. Методи захисту інформації. | **4/4** | | Захист практичної роботи. | **10** |

| | | | | |
|---|---|---|---|---|
| Тема 9. Задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в комп'ютерних системах. | **2/2** | | Захист практичної роботи. | **10** |
| Тема 10. Криптографічний захист інформації. | **4/4** | Вміти вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. | Захист практичної роботи. | **20** |
| **Самостійна робота** | | | | **20** |
| **Модульний контроль** | | | Підсумковий тест в ЕНК. | **30** |
| **Всього за 2 семестр** | | | | **70** |
| **Екзамен** | | | **Тест, теоретичні питання, задача** | **30** |
| **Всього за курс** | | | | **100** |

## ПОЛІТИКА ОЦІНЮВАННЯ

| | |
|---|---|
| ***Політика щодо дедлайнів та перескладання:*** | Дедлайни визначені в ЕНК. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний, стажування або відрядження). |
| ***Політика щодо академічної доброчесності:*** | Списування під час самостійних робіт, тестування та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). |
| ***Політика щодо відвідування:*** | Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній on-line формі за погодженням із деканом факультету). |

## ШКАЛА ОЦІНЮВАННЯ СТУДЕНТІВ

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

## РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ


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.