

Київський столичний університет імені Бориса Грінченка

Факультет журналістики

Кафедра реклами та зв'язків з громадськістю

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної
та навчальної роботи

О. Б. Жильцов

«_____» _____ 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Медіаіндустрія та медіабезпека: Медіабезпека

для здобувачів

спеціальності	061 «Журналістика»
рівня вищої освіти	першого (бакалаврського)
освітньої програми	061.00.02 «Реклама і зв'язки з громадськістю»

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
Програма № 0446/25
Научно-метод. відділ моніторингу якості освіти
(підпис) _____ (прізвище, ініціали)
«_____» _____ 2025 р.

Київ-2025

Розробник:

Харамурза Дар'я Вікторівна, доктор філософії з журналістики

Викладачі:

Кочубей Лариса Олександрівна, доктор політичних наук, професор, професор кафедри реклами та зв'язків з громадськістю;

Сінько Андрій Сергійович, викладач кафедри реклами та зв'язків з громадськістю.

Робочу програму розглянуто і затверджено на засіданні кафедри реклами та зв'язків з громадськістю

Протокол № 1 від 26 серпня 2025 року

Завідувач кафедри Ноборка Л. М. Новохатько

Робочу програму погоджено із гарантом освітньо-професійної програми з реклами та зв'язків з громадськістю

_____ 2025 року

Гарант освітньо-професійної програми Г. М. М. М. М. Нетреба

Робочу програму перевірено

_____ 2025 року

Заступник декана Факультету журналістики

з науково-методичної та навчальної роботи Д. В. Д. Р. В. Дьяченко

Пролонговано

на 20__/20__ н.р. підпис (ПІБ), «__»__20__ р., протокол № _____

на 20__/20__ н.р. підпис (ПІБ), «__»__20__ р., протокол № _____

на 20__/20__ н.р. підпис (ПІБ), «__»__20__ р., протокол № _____

на 20__/20__ н.р. підпис (ПІБ), «__»__20__ р., протокол № _____

1. Опис навчальної дисципліни.

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	основна	-
Мова викладання, навчання та оцінювання	українська	-
Загальний обсяг кредитів/годин	1/30	-
Курс	2	-
Семестр	3	-
Кількість змістових модулів з розподілом	1	-
Обсяг кредитів	1	-
Обсяг годин, в тому числі:	30	-
Аудиторні	14	-
Модульний контроль	2	-
Семестровий контроль	5	-
Самостійна робота	9	-
Форма семестрового контролю	екзамен	-

2. Мета та завдання навчальної дисципліни.

Мета дисципліни – формування у здобувачів системи знань з питань медіабезпеки, підготовка майбутніх фахівців реклами та зв'язків з громадськістю до роботи в умовах інформаційно-психологічних загроз, набуття практичних навичок та вмінь провадження безпечної медіадіяльності.

Завдання дисципліни розвивати наступні загальні та спеціальні компетентності:

- **ЗК 5.** Навички використання інформаційних і комунікаційних технологій.
- **ЗК 8.** Здатність навчатися і оволодівати сучасними знаннями.
- **ЗК 11.** Здатність спілкуватися державною мовою.
- **СК 2.** Здатність формувати інформаційний контент.
- **СК 6.** Здатність до провадження безпечної медіадіяльності та професійної дії в умовах кризових комунікацій.
- **СКУ 8.** Здатність володіти емоційним інтелектом в умовах професійної діяльності.

Діяльність (робота) здобувачів у Центрах компетентностей:

- Центр мультимедійних технологій;
- Інформаційно-аналітичний центр.

3. Результати навчання за дисципліною.

- **РН 5.** Використовувати сучасні інформаційні й комунікаційні технології та спеціалізоване програмне забезпечення для вирішення професійних завдань.
- **РН 8.** Виокремлювати у виробничих ситуаціях факти, події, відомості, процеси, про які бракує знань, і розкривати способи та джерела здобування тих знань.
- **РН 11.** Вільно спілкуватися з професійних питань, включаючи усну, письмову та електронну комунікацію, українською мовою.
- **РН 14.** Генерувати інформаційний контент за заданою темою з використанням доступних, а також обов'язкових джерел інформації.
- **РН 18.** Використовувати необхідні знання й технології для виходу з кризових комунікаційних ситуацій на засадах толерантності, діалогу й співробітництва.
- **РНУ 21.** Володіти емоціями з метою збереження емоційного балансу і налаштованості на позитивний результат в умовах професійної діяльності.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

№ з/п	Назви модулів і тем	Кількість годин						
		Разом	Аудиторних	Лекцій	Практичних	Семінарських	Самостійної роботи	МК / семестровий контроль
Модуль І.								
МЕДІАБЕЗПЕКА В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ								
1	Засади медіабезпеки	6	4	2		2	2	
2	Загрози для комунікації в медіапросторі	10	6	2	2	2	4	
3	Правила та принципи медіабезпеки	7	4	2	2		3	
	Модульний контроль	2	2 /					
	Разом за модулем І	25	14	6	4	4	9	2 /
	Екзамен	5						/ 5
	Разом за навчальним планом	30	14	6	4	4	9	2 / 5

5. Програма навчальної дисципліни

Модуль І. Медіабезпека в сучасному інформаційному просторі

Тема 1. Засади медіабезпеки

Поняття медіабезпеки. Основні принципи медіабезпеки. Поняття цифрової безпеки. Загрози в онлайн-просторі. Оцінка ризиків у цифровому просторі. Цифрова безпека медійника. Застосунки з цифрової безпеки. Безпечне

використання гаджетів. Захист даних. Медіабезпека в умовах війни та кризових ситуаціях.

Тема 2. Загрози для комунікації в медіапросторі.

Безпека комунікації в соціальних мережах і месенджерах «Фейсбук», «Вайбер», «Телеграм», «Ютуб». Небезпеки та загрози цифрових платформ («Гугл», «Вікіпедія»). Отримання даних користувачів в обхід цифрових платформ. Політика приватності використання сайтів та соціальних мереж. Інформаційні пастки у медіапросторі. Фішинг. Специфіка комунікації в мережі. Боти. Основні типи ботів. Сайти-сміттярки. Шкідливі блогери та псевдоексперти в медіапросторі. Як розпізнати шкідливого блогера та псевдоексперта. Маніпуляція аудиторією на цифрових платформах. Ознаки шахрайства, маніпуляцій у медіапросторі. Інструменти шахраїв, маніпуляторів і псевдоекспертів. Загрози інформаційного тероризму в медіапросторі. Загрози інформаційної безпеки.

Тема 3. Правила та принципи медіабезпеки.

Базові правила інформаційної гігієни. Безпечне споживання інформації. Сфери з найвищим ризиком шахрайства в медіапросторі. Безпечний пошук інформації з фінансових, економічних і політичних питань. Основні корисні ресурси з медіабезпеки та медіаграмотності. Методи та інструменти ідентифікації достовірності інформації в медіапросторі. Оптимізація безпеки даних пристроїв та сервісів. Захист облікових записів. Захист комунікації в мережі. Захист інформації на пристроях. Практичні поради та кейси з цифрової безпеки.

6. Контроль навчальних досягнень

За наявності сертифікатів проходження курсів, що відповідають тематичному блоку змістового модуля курсу, здобувачам можуть бути зараховані результати неформальної освіти.

Рекомендовані курси:

1) Цифрова безпека журналістів та інших працівників медіа
https://apps.prometheus.org.ua/learning/course/course-v1:Prometheus+DSJ101+2022_T1/home

2) Інформаційна безпека
https://apps.prometheus.org.ua/learning/course/course-v1:Internews+INFOS101+UA_2021_T3/home

6.1. Система оцінювання навчальних досягнень здобувачів

Вид діяльності здобувача	Максимальна кількість балів за одиницю	Модуль I	
		кількість одиниць	максимальна кількість балів
Відвідування лекційного заняття	1	3	3
Відвідування семінарського заняття	1	2	2
Робота на семінарському занятті	10	2	20
Відвідування практичного заняття	1	2	2
Робота на практичному занятті	10	2	20
Виконання завдань для самостійної роботи	5	2	10
Виконання модульної роботи	25	1	25
Разом			82
Максимальна кількість балів	82 бали		
Розрахунок коефіцієнта			
Розрахунок: 82 : 60 = 1,43			
Здобувач набрав: 76 балів			
Оцінка: 76 : 1,43 = 53 бали + бази за екзамен			

6.2. Завдання для самостійної роботи та критерії її оцінювання

Модуль I. Медіабезпека в сучасному інформаційному просторі Самостійна робота 1

Завдання

- Опишіть випадок цифрового шахрайства або фішингу, який стався з вами або вашими знайомими.
- Як цього можна було уникнути?

Самостійна робота 2

Завдання

Підготувати відповідь на питання.

- 2.1. Яких правил та принципів медіабезпеки ви дотримуетесь? Пояснити.
- 2.2. Які цифрові платформи на вашу думку є найбільш небезпечними для користувачів? Чому?

Оцінювання самостійної роботи здійснюється за такими *критеріями*:

- ступінь засвоєння фактичного матеріалу, який вивчається;
- ознайомлення з базовою та додатковою рекомендованою літературою;
- уміння поєднати теорію з практикою при розгляді конкретних ситуацій, розв'язанні завдань, винесених для самостійного опрацювання, і завдань, винесених на розгляд в аудиторії;
- логіка, структура, стиль викладу матеріалу в письмовій роботі, уміння

обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки;

- 5) повнота відповіді на питання, якість і самостійність виконання завдання; творчий підхід й ініціативність у виконанні завдання.

6.3. Форми проведення модульного контролю та критерії оцінювання

Модульна контрольна робота проводиться після вивчення певного змістового модуля. Оцінюється за виконання завдань у формі, зазначеній викладачем у робочій програмі. Виконання модульних контрольних робіт здійснюється у *формі* тестування та виконання практичних завдань. Такий формат дозволить визначити ступінь засвоєння теоретичного матеріалу кожного модуля та набутий рівень практичних навичок.

Кількість модульних контрольних робіт з навчальної дисципліни – 1, виконання кожної роботи є обов’язковим.

Критерії оцінювання:

- 1) розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються;
- 2) ступінь засвоєння фактичного матеріалу, який вивчається;
- 3) ознайомлення з базовими та додатковими рекомендованими джерелами;
- 4) уміння наводити й аналізувати приклади з медіаіндустрії, реклами та PR;
- 5) уміння поєднати теорію з практикою при розгляді конкретних ситуацій, розв’язанні завдань;
- 6) логіка, структура, стиль викладу матеріалу в письмових роботах і під час виступів в аудиторії, уміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки;
- 7) повнота відповіді на питання, якість і самостійність виконання завдання; творчий підхід й ініціативність у виконанні завдання.

При оцінюванні модульної контрольної роботи враховується обсяг і правильність виконаних завдань. Правильне виконання всіх завдань в межах однієї модульної роботи оцінюється максимально 25 балами.

6.4. Форми проведення семестрового контролю та критерії оцінювання

Семестровий контроль є результатом вивчення кожного модуля, який містить підсумок усіх форм поточного контролю та виконання модульної контрольної роботи. Семестровий контроль включає бали за поточну роботу здобувача на практичних, семінарських заняттях, виконання самостійної роботи, модульної контрольної роботи. Семестровий контроль знань проводиться у формі заліку й здійснюється по завершенні вивчення навчального матеріалу за результатами накопичених балів поточної роботи.

6.5. Шкала відповідності оцінок

Оцінка	Кількість балів	Рейтингова оцінка
Відмінно	100 – 90	A
Дуже добре	82 – 89	B
Добре	75 – 81	C
Задовільно	69 – 74	D
Достатньо	60 – 68	E
Незадовільно з можливістю повторного складання	59 – 35	FX
Незадовільно з обов'язковим повторним вивченням дисципліни	34 – 0	F

7. Навчально-методична картка дисципліни «Медіаіндустрія і медіабезпека: Медіабезпека»

Разом: 30 год., лекції – 6 год., семінарські заняття – 4 год., практичні заняття – 4 год., самостійна робота – 9 год., модульний контроль – 2 год., екзамен – 5 год.

Модулі	Модуль І		
Назва модуля	Медіабезпека в сучасному інформаційному просторі		
Кількість балів за модуль	82 бали		
Лекції	Відвідування – 3 б., з них:		
Теми лекцій	Засади медіабезпеки	Загрози для комунікації в медіапросторі	Правила та принципи медіабезпеки
Теми семінарських занять	Засади медіабезпеки 11 б.		Загрози для комунікації в медіапросторі 11 б.
Теми практичних занять	Загрози для комунікації в медіапросторі 11 б.		Правила та принципи медіабезпеки 11 б.
Самостійна робота	Самостійна робота 1, 2 – 10 б.		
Види поточного контролю	Модульна контрольна робота № 1 – 25 б.		
Підсумковий контроль	Всього балів – 82 бали		

8. Рекомендовані джерела

Основні джерела:

1. Індекс медіаграмотності українців: 2020–2022. Reporters sans frontières (France). URL: <https://detector.media/infospace/article/210209/2023-04-18-indeks-mediagramotnosti-ukraintsiv-2020-2022-kоротка-prezentatsiya/> (дата звернення: 15.08.2025).
2. Інформаційно-комунікаційна безпека: сучасні тренди : моногр. / Бровко О. О. [та ін.] ; за заг. ред.: Курбан О. В., Лісневська А. Л. Київ : Київ. ун-т ім. Б. Грінченка, 2022. 392 с.
3. Мороз О. Як не стати овочем. Інструкція з виживання в інфопросторі. Харків : Vivat, 2021. 256 с.
4. Посібник з безпеки для журналістів : посібник для репортерів у небезпечних зонах. Reporters sans frontières (France). 2022. 155 с. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381168> (дата звернення: 15.08.2025).
5. Kochybei Larysa, Radchenko Oksana, Nekryach Anastasia, , Michalski Tomash, Berezhnyi Yurii (2023). Comparative Analysis of Conceptual Models of Power Legitimation in Authoritarian, Democratic and Transitional Societies. *National Security Drivers of Ukraine. Information Technology, Strategic Communication, and Legitimacy* : Monograph. Cham: Springer, 186-201. <https://www.springer.com/series/11829> (Scopus)
6. Кочубей Л.О., Шевченко М.М. Інформаційні агенції: зарубіжний досвід для України. *Держава і право* : Збірник наукових праць. Юридичні і політичні науки. Випуск 97 / Ін-т держави і права імені В. М. Корецького НАН України. Київ: Вид-во «Юридична думка», 2025. С. 212-221. DOI: 10.33663/1563-3349-2025-97-212 (фахове видання, категорія «Б»). URL: <https://derzhava-i-pravo.com.ua/articles/97-212.pdf> (дата звернення: 15.08.2025).

Додаткові джерела:

1. Головка О. М. Медіабезпека людини: засади інформаційно-правової політики : монографія. Київ : Видавничий дім «АртЕк», 2019. 168 с.
2. Золотар О. О. Поняття та зміст категорії «інформаційна безпека людини». *Інформація і право*. 2021. № 1 (36). С. 73-78. URL: [https://doi.org/10.37750/2616-6798.2021.1\(36\).238185](https://doi.org/10.37750/2616-6798.2021.1(36).238185) (дата звернення: 15.08.2025).
3. Зражевська Н.І. Медіа як інструмент медіаконтролю і як засіб соціального примусу. *Держава та регіони. Серія соціальні комунікації*. 2022. Вип. 1(49). С. 122-129. URL: http://www.zhu.edu.ua/journal_cpu/index.php/der_sc/article/viewFile/892/869 (дата звернення: 15.12.2024).
4. Ілюк К. Інфодемія в українському телеграмі: хто, як та навіщо? Дослідження «Детектора медіа». URL: <https://detector.media/monitorynh-internetu/article/185330/2021-02-28-infodemiya-v-ukrainskomu-telegrami-khto-yak-ta-navishcho-doslidzhennya-detektora-media/> (дата звернення: 15.08.2025).
5. Курбан О. В. Інформаційні війни у соціальних он-лайн-мережах :

- монографія. Київ : Київ. ун-т ім. Б. Грінченка, 2017. 392 с.
6. Почепцов Г. Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2015. 497 с.
 7. Тексти.org.ua. URL: <https://texty.org.ua/> (дата звернення: 15.08.2025).
 8. Типи шахрайства. *Western Union*. URL: <https://www.westernunion.com/ua/uk/fraudawareness/fraud-types.html> (дата звернення: 15.08.2025).
 9. Харамурза Д. Інформаційний тероризм як інструмент гібридної війни та фактор руйнації медіапростору. *Інтегровані комунікації*. 2023. Вип. 2 (16). С. 29–37. URL: <https://doi.org/10.28925/2524-2644.2023.163> (дата звернення: 15.08.2025).
 10. Як? Практичні поради з цифрової безпеки. *Цифролаб*. URL: <https://yak.dslua.org/> (дата звернення: 15.08.2025).