Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Кафедра прикладної соціології та соціальних комунікацій

«ЗАТВЕРДЖУЮ»

Проректор з науково-педагогічної роботи

Олександр ГОЛОВКО

_____

_____ 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Безпека інформаційно-комунікативного простору цифрового суспільства»

(назва навчальної дисципліни)

рівень вищої освіти другий (магістерський) рівень вищої освіти

галузь знань 06 – Журналістика

спеціальність 061 Журналістика

освітня програма Стратегічні комунікації та нові медіа

спеціалізація _____

вид дисципліни вибіркова

факультет соціологічний

2022/2023 навчальний рік

Програму рекомендовано до затвердження вченою радою соціологічного факультету Харківського національного університету імені В.Н.Каразіна

«__15__» __червня_____2022 року, протокол №__7___

РОЗРОБНИКИ ПРОГРАМИ: (вказати авторів, їхні наукові ступені, вчені звання та посади)
Субота Марина Миколаївна, кандидат соціологічних наук, доцент кафедри прикладної соціології та соціальних комунікацій Харківського національного університету імені В.Н. Каразіна

Програму схвалено на засіданні кафедри прикладної соціології та соціальних комунікацій соціологічного факультету ХНУ імені В.Н.Каразіна

Протокол від «__27___» _____квітня_____2022 року №___3__

В.о. завідувача кафедри _____Віль БАКІРОВ

Гарант освітньої (професійної) програми «Стратегічні комунікації та нові медіа»


Вікторія БОЛОТОВА

Програму погоджено науково-методичною комісією соціологічного факультету Харківського національного університету імені В.Н. Каразіна

Протокол від «__21___» ___червня_____2022 року №_10_____

Голова науково-методичної комісії_  Юлія СОРОКА

ВСТУП

Програма навчальної дисципліни «Безпека інформаційно-комунікативного простору цифрового суспільства» складена відповідно до освітньо-професійної програми підготовки другого (магістерського) рівня вищої освіти Освітньої програми «Стратегічні комунікації та нові медіа» соціологічного факультету спеціальності 061 Журналістика

1. Опис навчальної дисципліни

1. Метою вивчення дисципліни «Безпека інформаційно-комунікативного простору цифрового суспільства» є формування у фахівців з інфомедійних технологій здатностей ідентифікувати соціально-небезпечний контент, протидіяти ворожим інформаційним і комунікативним атакам, дотримуватися професійних етичних норм, заснованих на цінностях громадянського (вільного демократичного) суспільства, аналізувати свою і чужу діяльність у просторі цифрових медіа.

2. Основними завданнями вивчення дисципліни є ознайомлення студентів із:

- на міждисциплінарних засадах (соціології, психології, теорії комунікації, теорії інформаційних війн тощо) забезпечити системне розуміння того, у який спосіб сучасні медіа формують сприйняття реальності та конструюють її, як здійснюється маніпуляція свідомістю користувачів медіа (і споживачів, і творців медійного контенту);
- ознайомити з основними концепціями відносно інформаційної і комунікативної безпеки у сучасному цифровому соціумі;
- вивчити способи розпізнання конкретних методик і прийомів маніпуляції, інформаційних і комунікативних атак, що застосовуються у соціальних комунікаціях цифрового суспільства;
- розвинути практичні навички критичного сприйняття, аналізу і перевірки інформації;
- сформувати поглиблені, практико-орієнтовані уявлення про сутність та шляхи забезпечення інформаціної безпеки у глобальних, локальних, внутрішньогрупових та міжособистісних медіакомунікаціях цифрового суспільства.

3. Кількість кредитів - 4,

4. Загальна кількість годин - 120 д.в., з них аудиторних – 36 (д.в.).

1.5. Характеристика навчальної дисципліни	
Обов'язкова / за вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	1-й
Семестр	
2-й	2-й
Лекції	
16 год.	4 год.
Практичні, семінарські заняття	
16 год.	6 год.
Лабораторні заняття	

Самостійна робота	
88 год.	110 год.
у тому числі індивідуальні завдання	
-	

1.6 Заплановані результати навчання:

Згідно з вимогами освітньо-професійної програми, здобувачі повинні набути компетентності та демонструвати такі результати навчання:
Перелік предметних компетентностей здобувача вищої освіти:

Загальні компетентності:

ЗК 1 – Здатність до абстрактного та конкретного мислення, аналізу та синтезу, здатність оперувати теоретичними положеннями, категоріями та поняттями.
ЗК 2 – Вміння виявляти, ставити та вирішувати проблеми.
ЗК 3 – Розвинене креативне мислення, творче і нестандартне ставлення до професійних завдань, здатність генерувати нові ідеї та рішення, креативно застосовувати теоретичні знання у практичних ситуаціях.
ЗК 4 – Здатність планувати час та управляти ним.
ЗК 5 – Здатність до пошуку, обробки й аналізу інформації з різних цифрових джерел.
ЗК 6 – Здатність до конструктивної критики та самокритики.
ЗК 7 – Здатність до аргументованого представлення власної думки, компетентної та толерантної дискусії з її опонентами.
ЗК 8 – Навички використання інформаційно-комп'ютерних комунікаційних технологій.
ЗК 11 – Здатність до міжособистісного спілкування, уміння працювати в команді, мотивувати людей та досягати спільної мети, розуміння та повага до різноманітності та мультикультурності.
ЗК 12 – Прагнення до саморозвитку, підвищення своєї професійної кваліфікації та майстерності.

Фахові компетентності:

ФК 1 – Здатність застосовувати соціологічні поняття, концепції та теорії для розуміння та адекватної інтерпретації проблемних соціальних явищ і процесів.
ФК 2 – Розуміння особливостей соціальних процесів, трендів, можливостей в Україні та світі в цифрову епоху.
ФК 3 – Здатність розробити програму емпіричного соціологічного дослідження в онлайн-форматі.
ФК 4 – Здатність застосувати соціологічний дослідницький інструментарій для проведення онлайн-досліджень.

ФК 5 – Здатність знаходити соціальну інформацію у відкритому доступі, у базах даних, здійснювати її змістовне структурування й узагальнення.

ФК 11 – Здатність використовувати на практиці теоретичні положення для аналізу та визначення ефективності проведення кампаній з застосуванням соціально-комунікативних технологій.
ФК 9 – Здатність ідентифікувати у комунікаційних системах соціально-небезпечний контент або ненормативну форму спілкування, вміння оперувати відповідними типологіями ризиків та небезпек.
ФК 10 – Здатність використовувати мультимедійні технології для презентації соціологічних досліджень, аналітичних матеріалів, комунікативного контенту.
ФК 11 – Здатність використовувати на практиці теоретичні положення для аналізу та визначення ефективності проведення кампаній з застосуванням соціально-комунікативних технологій.
ФК 12 – Здатність зіставити наявне знання з практичними викликами.

Програмні результати навчання:

ПРН 1 – Вміння застосовувати соціологічні поняття, концепції та теорії для пояснення особливостей функціонування та розвитку цифрового суспільства.
ПРН 2 – Вміння розробляти дизайн та інструментарій соціологічних онлайн-досліджень та презентувати їх результати.
ПРН 8 – Здатність здійснювати оперативне реагування на ризики та загрози недоброчесних комунікацій, протидіяти ворожим інформаційним атакам в контексті гібридних війн.
ПРН 11 – Формулювати дослідницькі запитання та конкретизовувати мету дослідження.
ПРН 12 – Визначати соціальні проблеми викликані цифрового соціуму, їх можливі структурні та культурні чинники.

2. Тематичний план навчальної дисципліни

Розділ 1. Концептуальні засади виявлення загроз інформаційній і комунікативний безпеці

Тема 1. Безпека інформаційно-комунікативного простору цифрового суспільства: базові поняття

Вступ до курсу. Організаційні питання. Зміст і завдання, організаційно-методичні особливості засвоєння курсу. Основна література. Міждисциплінарні засади вивчення предмету. Актуальність та практична значущість вивчення засад безпеки інформаційно-комунікативного простору цифрового соціуму. Сучасний розвиток інформаційно-комунікаційних та інформаційно-комунікативних технологій. Основні поняття курсу: інформаційний простір, комунікативний простір, інформаційно-комунікативний простір, медіапростір, інформаційна безпека, комунікативна безпека, кібербезпека, соціальна безпека, національна безпека, пропаганда, маніпуляція (прихований вплив). Концептуалізація наукових поглядів на проблему формування та забезпечення безпеки інформаційно-комунікативного простору. Сутність і поняття інформаційної (інформаційно-психологічної) війни, інформаційно-психологічних операцій. Сутність комунікативної війни. Загальні особливості ведення інформаційних та комунікативних війн в умовах розвитку нових медіа. Базові прийоми та інструменти ведення сучасних інформаційних та комунікативних війн.

Тема 2. Психологічні засади впливу на індивідуальну, групову та масову свідомість

Психологічні та соціально-психологічні передумови маніпулятивної взаємодії. Маніпуляція на рівні психічних процесів: перцептивні, мнемотичні, інтелектуальні процеси, емоційна і когнітивна дія. Базові засади психології впливу.

Психоаналітичні засади маніпулятивних технологій. Технології, спрямовані на нейтралізацію психологічних механізмів захисту, приклади їхнього застосування, способи їхнього розпізнання та протидії. Технології впливу на підсвідомість, використання сублімінальних стимулів: правда та міфи. НЛП-технології як технології маніпулювання: правда та міфи. Змінені стани свідомості. Психологія натовпу. Маніпуляція, з використанням підсвідомих процесів, на рівні масової та групової свідомості.

Маніпуляції, що використовуються у тоталітарних сектах та деструктивних культах.

Біхевіористські засади маніпулятивних технологій. Основні біхевіористські принципи управління людською поведінкою, оперантне обумовлення та підкріплення реакцій. Приклади застосування подібних технологій в медіакомунікаціях.

Критика маніпуляції в гуманістичній психології (Карнегі vs. Антикарнегі).

Підхід когнітивної психології до розуміння маніпулятивного впливу. Когнітивні викривлення.

Тема 3. Соціосеміотичні аспекти маніпулятивного пливу

Ключові поняття семіотичного аналізу комунікації. Лігвістичні засоби і прийоми маніпулювання. Маніпулювання за допомогою візуальних образів як знаково-семіотичних систем. Меми у цифровому просторі як інструмент маніпуляції. Маніпуляція за допомогою ідеології як символічної системи репрезентації реальності. Маніпуляція і конструювання соціальної реальності. Дискурсивна концепція ідеології. Розуміння маніпуляції з позиції критичного-дискурс-аналізу. Концепція міфу за Р. Бартом, міф як засіб маніпулювання свідомістю: основні принципи, аналіз конкретних прикладів застосування. Риторичні прийоми маніпулятивної дії (метафора, алюзія тощо). Наратив як інструмент маніпуляції.

Розділ 2. Протидія загрозам інформаційній і комунікативній безпеці

Тема 4. Дослідницькі інструменти виявлення маніпуляцій у медіа

Контент-аналіз як метод дослідження змісту медіакомунікації. Семіотичний аналіз тексту. Структурний аналіз тексту. Дискурс-аналіз аналіз. Метод наративного аналізу. Застосування цих інструментів в кількісних, якісних і кількісно-якісних дослідженнях маніпуляцій у медіа.

Принципи та прийоми верифікації інформації в інтернеті. Фактчекінг у роботі фахівця з медіакомунікацій. Вітчизняний та міжнародний досвід практик фактчекінгу. Основні інструменти і платформи фактчекінгу.

Тема 5. Інформаційна безпека в контексті протидії маніпулятивним технологіям у масовій комунікації

Мас-медіа як суб’єкт маніпулювання індивідуальної та масовою свідомістю. Сучасні уявлення про ефективність масової комунікації. Медіа відображають чи створюють реальність? Специфічні медіа технології маніпулювання (завдання «порядку денного», праймінгу, конструювання соціальних проблем, «розкручування спіралі мовчання). Негативізм і сенсаціоналізм. Медіафреймінг як спосіб впливу на аудиторію.

Маніпулятивні технології, що застосовуються у рекламній комунікації (аналіз конкретних прикладів).

Тема 6. Протидія специфічним технологіям прихованого впливу в інтернет-комунікації

Інтернет як простір символічної політичної боротьби і застосування маніпулятивних технологій. Чому в умовах сучасного світу пропаганда є знову дієвою? Розподіл аудиторії в соціальних мережах. Психологія людини в соціальних мережах. Вибіркове сприйняття інформації (концепція когнітивного дисонансу). «Бульбашка фільтрів / інформаційна бульбашка». Мікротаргетинг як сучасна технологія маніпулювання в інтернет-комунікації.

Безпека в соціальних мережах. Кейси та інструменти захисту. Що таке постправда? Постправда як інструмент інформаційо-психологічних війн в умовах нових медіа. Феномен і поняття «фейк». Приклади (кейси) здійснення інформаційних атак у просторі соціальних медіа. Основні технології маніпулювання індивідуальною, груповою та масовою свідомістю в інтернет-комунікації.

Тема 7. Маніпулятивні технології у політичній комунікації

Маніпулятивні електоральні технології. Специфічні технології політичної реклами. Технологія встановлення «політичного порядку денного». Стериотипізація політичного дискурсу. Прийоми дифамації політичного супротивника. Критичний аналіз дискурсу політичної полеміки: на матеріалі мас-медіа.

Маніпуляції даними соціологічних досліджень. Маніпуляції статистичними даними.

3. Структура навчальної дисципліни

Назви розділів 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
Розділ 1. Безпека інформаційно-комунікативного простору цифрового суспільства: базові поняття												
Тема 1. Безпека інформаційно-комунікативного простору цифрового суспільства: базові поняття	16	2	2			12	16	0,5	0,5			15
Тема 2. Психологічні засади впливу на індивідуальну, групову та масову свідомість	16	2	2			12	16	0,5	0,5			15
Тема 3. Соціосеміотичні аспекти маніпулятивного пливу	16	2	2			12	16	0,5	1			14,5
Разом за розділом 1	48	6	6			36	48	1,5	2			44,5
Розділ 2. Протидія загрозам інформаційній і комунікативній безпеці												

Тема 4. Дослідницькі інструменти виявлення маніпуляцій у медіа	27	4	4			19	27	1	1			25
Тема 5. Інформаційна безпека в контексті протидії маніпулятивним технологіям у масовій комунікації	15	2	2			11	15	0,5	1			13,5
Тема 6. Протидія специфічним технологіям прихованого впливу в інтернет-комунікації	15	2	2			11	15	0,5	1			13,5
Тема 7. Маніпулятивні технології у політичній комунікації	15	2	2			11	15	0,5	1			13,5
Разом за розділом 2	72	10	10			52	72	2,5	4			65,5
Усього годин	120	16	16			88	120	4	6			110

4. Теми семінарських занять д.в

Назва теми	Кількість Годин
Тема 1. Безпека інформаційно-комунікативного простору цифрового суспільства: базові поняття	2
Тема 2. Психологічні засади впливу на індивідуальну, групову та масову свідомість	2
Тема 3. Соціосеміотичні аспекти маніпулятивного пливу	2
Тема 4. Дослідницькі інструменти виявлення маніпуляцій у медіа	4
Тема 5. Інформаційна безпека в контексті протидії маніпулятивним технологіям у масовій комунікації	2
Тема 6. Протидія специфічним технологіям прихованого впливу в інтернет-комунікації	2
Тема 7. Маніпулятивні технології у політичній комунікації	2
Разом	16

5. Завдання для самостійної роботи д.в

№ з/п	Види, зміст самостійної роботи	Кількість годин д.в
1	Прочитати літературні джерела з теми заняття. Підготовити відповіді на запитання до семінарського заняття. Написати есе.	12
2	Прочитати літературні джерела з теми заняття. Підготовити відповіді на запитання до семінарського заняття.	12

3	Прочитати літературні джерела з теми заняття. Подивитися документальний фільм за темою зайняттям Підготовити відповіді на запитання до семінарського заняття. Написати есе.	12
4	Прочитати літературні джерела з теми заняття. Підготовити відповіді на запитання до семінарського заняття. Підготовити відповіді на запитання до семінарського заняття. Розпочати виконання письмової практичної (дослідницької) роботи.	19
5	Прочитати літературні джерела з теми заняття. Подивитися художній фільм за темою заняття. Підготовити відповіді на запитання до семінарського заняття. Виконувати письмову практичну (дослідницьку) роботу. Пройти інтерактивну навчальну онлайн гру.	11
6	Прочитати літературні джерела з теми заняття. Подивитися художній фільм за темою зайняття. Підготовити відповіді на запитання до семінарського заняття. Написати есе. Виконувати письмову практичну (дослідницьку) роботу. Підготувати захист дослідницького проекту – самостійної роботи.	11
7	Прочитати літературні джерела з теми заняття. Підготовити відповіді на запитання до семінарського заняття. Підготувати захист дослідницького проекту – самостійної роботи.	11
	Разом	88

6. Види навчальної діяльності (змішане навчання, лекції, семінарські заняття)

Тема	**Класифікація**	**Попередня підготовка**	**Подача нової інформації**	**Тренування**	**Зворотній зв'язок**
Розділ 1. Безпека інформаційно-комунікативного простору цифрового суспільства: базові поняття					
Тема 1. Безпека інформаційно-комунікативного простору цифрового суспільства: базові поняття	Вступна лекція, семінар	Ознайомлення або повторення термінології, необхідної для роботи з темою	Презентація відеоконференція	Робота з літературою	Обговорення навчального матеріалу (Групові консультації; коментарі під час заняття від викладача)
Тема 2. Психологічні засади впливу на індивідуальну, групову та масову свідомість	Інформаційна лекція, семінар	Ознайомлення або повторення термінології, необхідної для роботи з темою	Презентація Відеоконференція. Документальній фільм за проблемним питанням лекції.	Робота з літературою Робота з кейсами;	Обговорення навчального матеріалу (Групові консультації; коментарі під час заняття від викладача)

Тема 3. Соціосеміотичні аспекти маніпулятивного пливу	Інформаційна лекція, семінар	Ознайомлення або повторення термінології, необхідної для роботи з темою	Презентація відеоконференція	Робота з літературою Робота з кейсами;	Обговорення навчального матеріалу (Групові консультації; коментарі під час заняття від викладача) Завдання у Classroom
Розділ 2. Протидія загрозам інформаційній і комунікативній безпеці					
Тема 4. Дослідницькі інструменти виявлення маніпуляцій у медіа	Інформаційна лекція, семінар	Ознайомлення або повторення термінології, необхідної для роботи з темою	Презентація Відеоконференція робота в групах	Робота з літературою Робота з кейсами;	Обговорення навчального матеріалу (Групові консультації; коментарі під час заняття від викладача)
Тема 5. Інформаційна безпека в контексті протидії маніпулятивним технологіям у масовій комунікації	Інформаційна лекція, семінар	Ознайомлення або повторення термінології, необхідної для роботи з темою	Презентація Відеоконференція, робота в групах. Інтеративна навчальна онлайн гра. Художній фільм за проблемним питанням лекції.	Робота з літературою Робота з кейсами;	Обговорення навчального матеріалу (Групові консультації; коментарі під час заняття від викладача) Завдання у Classroom
Тема 6. Протидія специфічним технологіям прихованого впливу в інтернет-комунікації	Інформаційна лекція, семінар	Ознайомлення або повторення термінології, необхідної для роботи з темою	Презентація Відеоконференція. Художній фільм за проблемним питанням лекції.	Робота з літературою Робота з кейсами;	Обговорення навчального матеріалу (Групові консультації; коментарі під час заняття від викладача) Завдання у Classroom

Тема 7. Маніпулятивні технології у політичній комунікації	Підсумкова лекція, семінарське заняття	Ознайомлення або повторення термінології, необхідної для роботи з темою	Презентація відеоконференція	Робота з літературою Робота з кейсами;	Захист дослідницьких проектів

6. Індивідуальні завдання

-

7. Методи навчання

- **лекції** – розкриваються принципові та найбільш важливі аспекти визначених тем дисципліни із застосуванням мультимедійних засобів навчання. Застосовуються метод активізації навчально-пізнавальної діяльності студента з дисципліни (зокрема аналіз кейсів з історичної та сучасної практики застосування інформаційно-психологічних операцій, маніпулятивних технологій у медіакомунікаціях), метод проблемного викладу матеріалу. частково-пошуковий, або евристичний, метод, які орієнтуються на компетентнісний підхід в навчанні.

– **семінари** з елементами дискусії, ділової гри, підготовка презентаційних матеріалів, виступи опрацювання навчальної та наукової літератури, групо Робота направлена на збудження запитаннями інтересу до теми, створення мотивації навчання, розвиток пізнавальної активності, комунікативних умінь та навичок

- **самостійна робота** – поглиблене самостійне здобування знань (конспектування, тезування, анотування, рецензування, тощо), перегляд та аналіз художніх фільмів; удосконалення вмінь та навичок включає вивчення додаткової літератури та написання доповідей та есеїв, емпіричної дослідницької роботи.

-

8. Методи контролю

Контрольна робота, семінарські заняття, екзамен

Поточний контроль – усні опитування на лекціях та семінарських заняттях за контрольними та програмними питаннями поточної та попередніх тем; оцінювання ступеню активності студентів та якості їхніх виступів та коментарів при проведенні дискусій та інших видах роботи на семінарських заняттях (рольові ігри, командна робота, дискусії). Передбачена контрольна робота Самостійні роботи з теоретичних питань нормативного або проблемного характеру, письмові есе, *Рубіжний контроль* – контрольна робота за темами розділів. *Підсумковий контроль* – письмовий залік (три відкритих запитання проблемного характеру).

Критерії оцінювання питання контрольної роботи

Робота містить 3 відкритих питання, кожне з яких оцінюється максимум у 6 балів

Відповідь повна, або з однією незначною помилкою (ґрунтовна, аргументована, логічно побудована, містить посилання на конкретні приклади)	6 балів

Відповідь повна, але з двома-трьома незначними помилками (цілому вірна та повна, але містить окремі неточності або невеликі логічні протиріччя)	5-4 бали
Відповідь не досить повна, та (або) із суттєвими помилками (відповідь в цілому адекватна завданню, але є досить поверхневою та неповною)	3-2 бали
Відповідь не повна, містить суттєві помилки (відповідь не є адекватною завданню, але демонструє деякі знання матеріалу курсу, окремі згадки про важливі ідеї та концепції)	1 бал
Відповідь майже відсутня та (або) не відповідає запитанню	0 балів

Критерії оцінювання самостійної практичної (дослідницької) роботи:

1. змістовна відповідність завданню, використання матеріалів курсу – 4 бали;
2. коректність та глибина здійсненого аналізу – 4 бали;
3. обґрунтування результатів та висновків дослідження – 4 бали;
4. оформлення згідно вимог – 2 бал.

5.мультимедійна презентація – 4 бали

Максимальна кількість балів –18.

Критерії оцінювання роботи на семінарських заняттях:

Кількість балів, яку може отримати студент за усну та письмову роботу на семінарі становить від **2** до **4 балів**. Для цього необхідно продемонструвати володіння матеріалами теми, вміння аналізувати ключові аспекти теми, продемонструвати можливості їхнього застосування на практиці, а також виконання самостійних завдань за планом.

Критерії оцінювання письмового заліку:

З відкритих запитання, перше оцінюється у 14 балів, друге та третє – у 13

При оцінюванні враховується: правильність відповіді, її аналітичний характер, наведення прикладів, концептуальна відповідність (вміння оперувати категоріальним апаратом курсу).

Відповідь повна, або з однією незначною помилкою (ґрунтовна, логічно побудована, містить посилання на авторитетні джерела та на конкретні приклади)	13-14 балів
Відповідь повна, але з двома-трьома незначними помилками (цілому вірна та повна, але містить окремі неточності або невеликі логічні протиріччя)	10-12 балів
Відповідь не досить повна, та (або) із суттєвими помилками (відповідь в цілому адекватна завданню, але є досить поверхневою та неповною)	6-9 балів
Відповідь не повна, містить суттєві помилки (відповідь не є адекватною завданню, але демонструє деякі знання матеріалу курсу, окремі згадки про важливі ідеї та концепції)	2-5 балів
Відповідь майже відсутня та (або) не відповідає запитанню	0-1 балів

8.1 **Схема нарахування балів**

Поточний контроль та самостійна робота							Контрольна робота передбачена навчальним планом	Разом	залік	Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7				
4	4	4	18	4	4	4	18	60	40	100

Шкала оцінювання результатів навчання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для дворівневої шкали оцінювання
90 – 100	зараховано
70 – 89	зараховано
50 – 69	зараховано
1– 49	не зараховано

9. Рекомендована література

Основна література

1. Климанська Л. Д. Соціально-комунікативні технології в політиці: Таємниці політичної кухні : монографія / Л. Д. Климанська. – Львів : Видавництво Національного університету «Львівська політехніка», 2007. – 332 с.
2. Кулеба Д. Війна за реальність*:* як перемагати у світі фейків, правд і спільнот / Дмитро Кулеба. – Київ : Книголав, 2019. – 384 с.
3. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі: навч. посіб. / О. В. Курбан. – К. : ВІКНУ, 2016. – 286 с.
4. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Макименко, В. М. Желіховський. – Київ : КНТ, 2006. – 280 с.
5. Медіаосвіта та медіа грамотність : підручник / ред.-упор. В. Ф. Іванов, О. В. Волошенюк ; за науковою редакцією В. В. Різуна. – Київ : Центр Вільної Преси, 2013. – 352 с.
6. Парахонський Б. О., Яворська Г. М. Онтологія війни і миру: безпека, стратегія, смисл. – Київ : НІСД, 2019. – 560 с.
7. Татенко В.О. Соціальна психологія впливу: Монографія. – К.: Міленіум, 2008. – 216 с.
8. Andress J. The Basics of Information Security Understanding the Fundamentals of Infosec in Theory and Practice (Second Edition) / Jason Andress : Elsevier, 2014. – 240 p.
9. Whitman M. E. Management of Information Security. Fivth edition / M. E. Whitman, H. J. Mattord. – USA : Cengage Learning, 2017. – 568 p.

Допоміжна література

1. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О.Г. Додонов, Д.В. Ланде. – Київ: Інтертехнологія, 2009. – 164 с.
2. Дзьобань О. П. Інформаційна безпека у проблемному полі соціокультурної реальності: монографія. – Х. : Майдан, 2010. – 260 с.
3. Інформаційний простір України: четвертий рік війни [Електронний ресурс] // Інститут демократії імені Пилипа Орлика. – Режим доступу : http://idpo.org.ua/analitics/1385-informacijnij-prostir-ukra%D1%97ni-chetvertij-rik-vijni-pre zentaciya.html#comment-1561
4. Крос К. Політична комунікація і висвітлення новин у демократичних суспільствах: конкуруючі перспективи / Крос Кетлін, Гакет Роберт ; пер. Руслан Ткачук. – К. : Основи, 2000. – 142 с.
5. Лалл Дж. Мас-Медіа, комунікація, культура : глобальний підхід / Джеймс Лалл ; за ред. О. Гриценка, Н. Гончаренко ; пер. з англ. О. Гриценка, С. Гарастович, Т. Гарастович [та ін.]. – К. : К.І.С., 2002. – 264 с.
6. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / Валентин Петрик [сайт]. – Режим доступу :www.justinian.com.ua/article.php.
7. Полянський П. Освіта як об’єкт інформаційної війни Росії проти України і як ресурс протидії такій війні [Електронний ресурс] / П. Полянський. — Режим доступу : maidanua.org/2015/03.
8. Потеряхін А. Л. Інформаційно-психологічний вплив: визначення поняття / А. Л. Потеряхин // Інформаційна безпека людини, суспільства, держави. – 2009. – №2 (2). – С. 28–32.
9. Почепцов Г. Від покемонів до гібридних війн: нові комунікативні технології XXI століття / Георгій Почепцов. – Київ : Києво-Могилянська академія, 2017. – 258 с.
10. Прибутько П.С. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах / П.С. Прибутько, І.Б. Лук’янець. – Київ: Вид. А. В. Паливода, 2007. – 252 с.
11. Протидія російській пропаганді та медіаграмотність: результати всеукраїнського опитування громадської думки. Аналітичний звіт. – К. : Детектор медіа, 2018. – 64 с.
12. Саєнко О. Г. Інформаційна війна як прояв інформаційного протиборства [Текст] / О. Г. Саєнко, С.Л. Степаниця // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2008. – Вип. 12. – С. 142–147
13. Сватко Я. Національна безпека України в умовах ведення інформаційних війн [Електронний ресурс] / Я. Сватко // Західна аналітична группа. – Режим доступу: http://zgroup.com.ua/print.php?articleid=1606.
14. У нас погані новини: http://texty.org.ua/d/2018/mnews/
15. Lakoff G., Johnson M. Metaphors We Live By / Lakoff, George; Johnson, Mark University of Chicago Press, 2003. – 256 p.
16. Layton T. P. Information Security: Design, Implementation, Measurement, and Compliance / T. P. Layton. – NW : Auerbach Publications, 2016. – 264 p.

Наукова періодика:

1. A linguistic/game-theoretic approach to detection/explanation of propaganda/ Arash Barfar // Expert Systems with Applications15 October 2021Volume 189 (Cover date: 1 March 2022) Article 116069.
2. A model for understanding new media literacy: Epistemological beliefs and social media use/ Ismail Celik, Hanni Muukkonen, Selcuk Dogan // Library & Information Science Research20 October 2021Volume 43, Issue 4 (Cover date: October 2021)Article 101125.
3. Analytic thinking reduces belief in conspiracy theories / Viren Swami, Martin Voracek, Adrian Furnham // CognitionDecember 2014Volume 133, Issue 3Pages 572-585
4. Beyond Misinformation: Understanding and Coping with the «Post-Truth» Era/ Stephan Lewandowsky, Ullrich K. H. Ecker, John Cook // Journal of Applied Research in Memory and CognitionDecember 2017Volume 6, Issue 4Pages 353-369.
5. Cause and Effect: On the Antecedents and Consequences of Conspiracy Theory Beliefs / Joseph Uscinski, Adam M. Enders, Justin Stoler // Current Opinion in PsychologyAvailable online 28 May 2022 In press, journal pre-proof Article 101364.
6. Computers in Human Behavior27 November 2021Volume 128 (Cover date: March 2022) Article 107121.
7. Deepfake forensics: Cross-manipulation robustness of feedforward- and recurrent convolutional forgery detection methods/ Frederic Chamot, Zeno Geradts, Evert Haasdijk // Forensic Science International: Digital Investigation21 March 2022.
8. Fake News: The narrative battle over the Ukrainian conflict / Irina Khaldarova & Mervi Pantti // Journalism Practice, Volume 10, 2016 - Issue 7
9. Fake news: Why do we believe it? / Catherine Beauvais // Joint Bone SpineAvailable online 4 March 2022In press, journal pre-proofArticle 105371.
10. History as a propaganda tool in Putin’s Russia / Miguel Vázquez Liñán // Communist and Post-Communist StudiesJune 2010Volume 43, Issue 2 Pages 167-178.
11. Makhashvili L. The Russian Information War and Propaganda Narratives in the European Union and the EU's Eastern Partnership Countries / L. Makhashvili // International Journal of Social Science and Humanity. – 2017. – Vol. 7, №. 5. – P. 309–313.
12. Multifaceted Nature of Social Media Content Propagating COVID-19 Vaccine Hesitancy: Ukrainian Case / Olena Zakharchenko, Roksolana Avramenko, Olha Trach // Procedia Computer Science 26 January 2022.
13. Pragmatic mechanisms of manipulation in Russian online media: How clickbait works (or does not) / Valentina Apresjan, Alexander Orlov // Journal of Pragmatics Available online 3 March 2022 In press, corrected proof.
14. Psychological benefits of believing conspiracy theories / Jan-Willem van Prooijen // Current Opinion in Psychology 5 May 2022Volume 47 (Cover date: October 2022) Article 101352.
15. Social Media Advertising through Private Messages and Public Feeds: A Congruency Effect between Communication Channels and Advertising Appeals / Fue Zeng, Ruijuan Wang, Zhe Qu // Information & Management 28 March 2022Volume 59, Issue 4 (Cover date: June 2022) Article 103646.
16. Social media and the future of open debate: A user-oriented approach to Facebook’s filter bubble conundrum / Philip Seargeant, Caroline Tagg // Discourse, Context & Media10 April 2018Volume 27 (Cover date: March 2019) P. 41-48.
17. Social network behavior and public opinion manipulation / Long Chen, Jianguo Chen, Chunhe Xia // Journal of Information Security and Applications8 December 2021Volume 64 (Cover date: February 2022) Article 103060.
18. Testing the cognitive involvement hypothesis on social media: 'News finds me' perceptions, partisanship, and fake news credibility/ Trevor Diehl, . Sangwon Lee //
19. The affective politics of the “post-truth” era: Feeling rules and networked subjectivity / Megan Boler, Elizabeth Davis // Emotion, Space and Society7 May 2018.

20. The anatomy of undue influence used by terrorist cults and traffickers to induce helplessness and trauma, so creating false identities /. S. A. Hassan, M. J. Shah // Ethics, Medicine and Public HealthJanuary–March 2019Volume 8Pages 97-107.
21. The dark side of social movements: social identity, non-conformity, and the lure of conspiracy theories / Anni Sternisko, Aleksandra Cichocka, Jay J Van Bavel // Current Opinion in Psychology21 February 2020Volume 35 (Cover date: October 2020) P. 1-6.
22. The impact of group polarization on the quality of online debate in social media: A systematic literature review / Luca Iandoli, Simonetta Primario, Giuseppe Zollo // Technological Forecasting and Social Change10 June 2021Volume 170 (Cover date: September 2021) Article 120924.
23. The responsibility of social media in times of societal and political manipulation / Ulrike Reisach // European Journal of Operational Research22 September 2020Volume 291, Issue 3 (Cover date: 16 June 2021) P. 906-917.
24. The spread of the Kremlin's narratives by a western news agency during the Ukraine crisis /. Kohei Watanabe // Journal of International Communication, Volume 23, 2017 - Issue 1
25. Who believes in conspiracy theories? A meta-analysis on personality correlates / Lukasz Stasielowicz, // Journal of Research in Personality4 April 2022 Volume 98 (Cover date: June 2022) Article 104229.
26. Дубас О. П. Інформаційно-комунікативний простір: поняття, сутність, структура / О. П. Дубас // Сучасна українська політика. Політики і політологи про неї. – К. : Український центр політичного менеджменту, 2010. – Вип. 19. – С. 223–232.
27. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення / Ю.О. Горбань // Вісник НАДУ. – 2015, №1. – С. 136–141.
28. Младьонова О. Д. Інформаційна безпека як складова національної безпеки України / О. Д. Младьонова // Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Питання політології». – 2017. – № 31. – С. 87–92.
29. Онищук М. І. Особливості психологічного впливу в ході проведення психологічних операцій/ М. І. Онищук, Я. М. Жарков // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2008. – Вип. 16. С. 136–139.
30. Павловська С. Інформаційно-психологічний вплив як фактор досягнення мети в ході воєнних дій / С. Павловська // Воєнна історія. – 2008. - №5. – С. 126-136
31. Побокін М. Маніпулятивний вплив в системі політичних технологій // Людина і політика 2004 № 3, С. 63-73.
32. Солдатенко І. О. Медіаграмотність як складова інформаційної безпеки / І. О. Солдатенко, А. В. Зінюк // Актуальні проблеми філософії та соціології. – 2016. – № 10. – С. 138–140.
35. Соснін О. В. Проблеми зростаючої ролі інформаційно-комунікаційної функції держави в умовах інформаційного суспільства та шляхи їх вирішення / О. В. Соснін // Гуманітарний вісник ЗДІА. Серія: Філософія. – 2016. – № 65. – С. 164–176.

36. Субота М. М. Комунікативна безпека / М. М. Субота // Електронна освіта : термінологічний словник / за ред. В. С. Бакірова. – Харків : Видавничий центр Харківського національного університету імені В. Н. Каразіна, 2016. – С. 99-100.
37. Субота М. М. Безпека даних / М. М. Субота // Електронна освіта : термінологічний словник / за ред. В. С. Бакірова. – Харків : Видавничий центр Харківського національного університету імені В. Н. Каразіна, 2016. – С. 13-14
38. Субота М. М. Особливості дискурсу теленовин у контексті медіаконструювання соціальної реальності // Український соціологічний журнал. 2011. №. 1-2. С. 48–55.
39. Субота М. М., Зінюк А. В. Проблема соціологічної концептуалізації поняття «інформаційна безпека держави» // Сучасні проблеми світового співтовариства та роль суспільних наук у забезпеченні його розвитку : матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 11-12 березня 2016 року). Одеса : ГО «Причорноморський центр досліджень проблем суспільства» . С. 92–94.

Нормативно-правова база

1. Проект Концепції інформаційної безпеки України [Електронний ресурс]. – Режим доступу : http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf
2. Закон України «Про державну службу спеціального зв'язку та захисту Інформації України» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/3475-15
3. Закон України «Про державну таємницю» // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С.252-276
4. Закон України «Про доступ до публічної інформації» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу http://zakon0.rada.gov.ua/laws/show/2939-17
5. Закон України «Про захист інформації в авторизованих системах» // Інформаційне законодавство: збірник законодавчих актів у 6 томах / за ред. Ю.С. Шемшученка . – т.1. - Інформаційне законодавство України. – К.: ТОВ «Юридична думка», 2005. – С. 277-282
6. Закон України «Про захист персональних даних» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2297-17
7. Закон України «Про науково-технічну інформацію» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon5.rada.gov.ua/laws/anot/3322-12
8. Закон України «Про Національну систему конфіденційного зв'язку» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/2919-14
9. Закон України «Про основи національної безпеки» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/964-15
10. Концепція національної безпеки України [Електронний ресурс] // Міністерство інформаційної політики України: [сайт]. - Режим доступу: http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%

96%D1%97%20%28%D0%A2%D0%B5%D0%BA%D1%81%D1%82%29%20-%2030.09.15.pdf

11. Указ Президента України «Про доктрину інформаційної безпеки України» [Електронний ресурс] // Верховна Рада України: [сайт]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009
12. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/472017-21374

12. Посиланная на інформаційні ресурси в Інтернеті, відеолекції, інше методичне забезпечення

1. Watchdog українських ЗМ (ГО «Детектор медіа» : Детектор медіа – українське інтернет-видання про медіа від команди Наталії Лигачової) – http://detector.media/
2. Детектор медіа. Моніторинг – https://detector.media/category/monitoring/
3. Проект MediaSapiens був започаткований«Телекритикою» (зараз – «Детектор медіа») у 2010 році за підтримки Інтерньюз-Нетворк (США) – http://osvita.mediasapiens.ua/ –
4. StopFake, волонтерський інтернет-проєкт – http://www.stopfake.org
5. TEXTY.org.ua – суспільно-політичне та аналітичне інтернет-видання – http://texty.org.ua/
6. Інститут масової інформації (IMI) (українська громадська організація) – https://imi.org.ua/
7. Незалежна аналітична платформа «Вокс Україна» (досліження) Електронний ресурс]. Режим доступу : https://voxukraine.org/doslidzhennya/
8. Академія української преси (Моніторинг) – http://www.aup.com.ua/
9. Проект «Українського кризового медіа-центру» – http://uchoose.info/
10. Онлайн-курс «Новинна грамотність» [Електронний ресурс]. Режим доступу : http://video.detector.media/special-projects/novynna-gramotnist-i22
11. Дистанційний навчальний курс медіаграмотності для громадян (створений IREX у партнерстві з Академією української преси та StopFake) – http://irex.mocotms.com/ml_web/story_html5.html
12. Дистанційний курс «Верифікація в Інтернеті» (розрахований на журналістів і редакторів пострадянського простору) – https://vumonline.ua/course/verification-in-the-Internet/
13. Освітній проект «OSINT Academy» від Інституту постінформаційного суспільства (курс дає розуміння базових інструментів розвідки з відкритих джерел і розрахований на журналістів, блогерів, громадських активістів, представників прес-служб і всіх, хто створює і поширює контент з важливих для українського суспільства питань) – http://www.osint.academy/
14. Дистанційний курс «Як розуміти соціальні мережі» – https://vumonline.ua/course/how-to-understand-social-networks/
15. Мультимедійний онлайн-посібник «МедіаДрайвер» (від Детектор Медіа) – http://mediadriver.online/
16. Видання «Як розпізнати фейк?» (від Міністерства інформаційної політики України, розроблене та реалізоване спільно з проектом ЄС «Association4U») – http://mip.gov.ua/files/pdf/antifake_ua_web.pd
17. Фактчекінгова організація (США) PolitiFact National – https://www.politifact.com/truth-o-meter/
18. Фактчекінговий проект The Washington Post https://www.washingtonpost.com/news/fact-checker/?utm_term=.129394214c9b
19. The Fact Checker (The Gazette) – https://www.thegazette.com/fact-checker/
20. Фактчекінговий проект про погоду та зміну клімату Climate Feedback – https://climatefeedback.org/